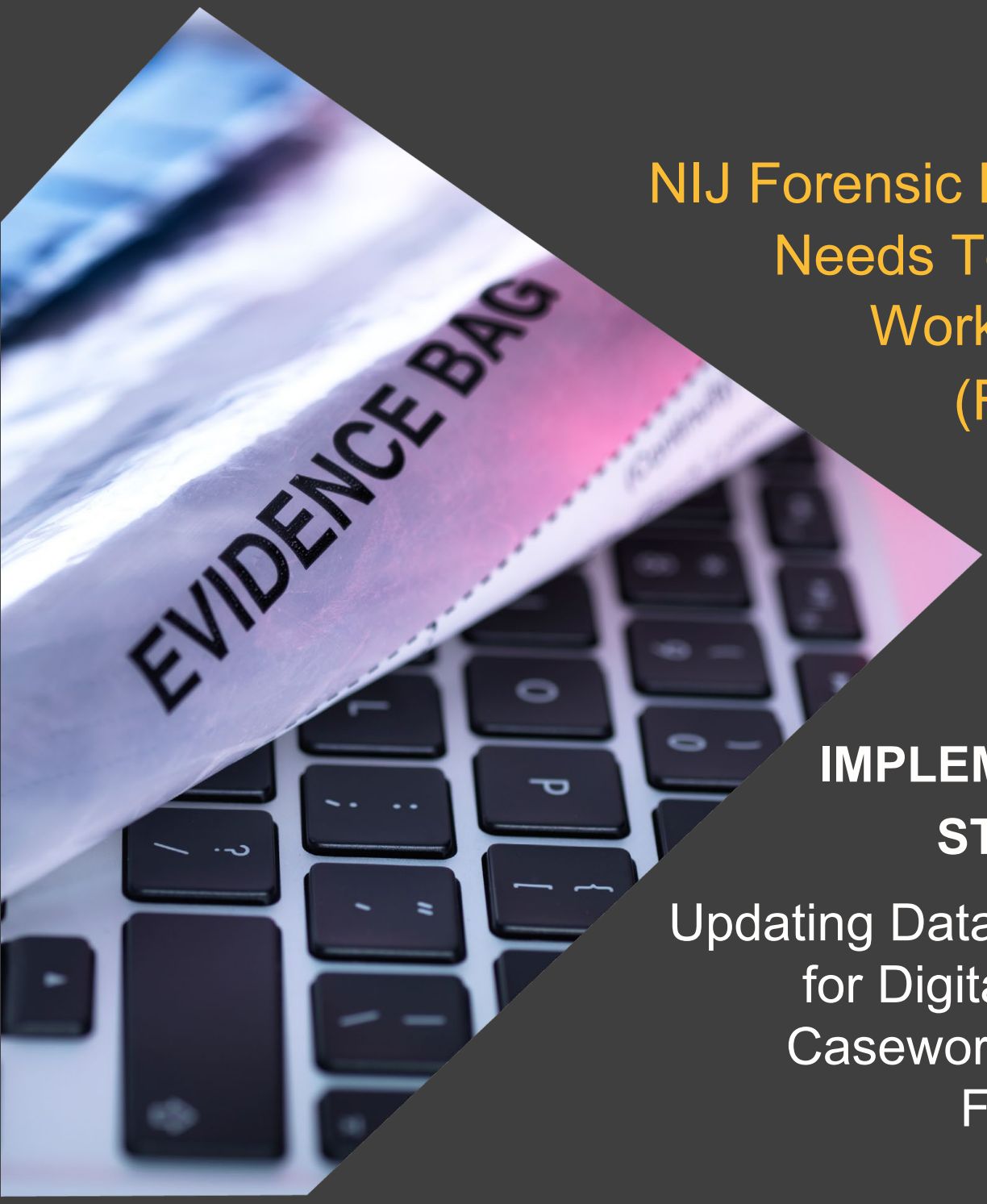

NIJ Forensic Laboratory Needs Technology Working Group (FLN-TWG)

IMPLEMENTATION STRATEGIES

Updating Data Collection for Digital Evidence Casework in Project FORESIGHT

August 2022

The Forensic Laboratory Needs Technology Working Group (FLN-TWG) developed this Implementation Strategies. The FLN-TWG is an activity administered under the National Institute of Justice (NIJ) Forensic Technology Center of Excellence (FTCoE) program. RTI International leads the FTCoE, which is supported through an NIJ Cooperative Agreement (2016-MU-BX-K110), Office of Justice Programs, U.S. Department of Justice (DOJ). Any opinions or points of view expressed in this white paper are those of the FLN-TWG and do not necessarily reflect the official position or policies of NIJ or the DOJ.

Table of Contents

Exhibits

I. Topic/Technology: Project FORESIGHT Overview

Project FORESIGHT is a business-guided self-evaluation of forensic science laboratories across the globe. The participating laboratories represent metropolitan, regional, state, and national agencies. Faculty from the West Virginia University John Chambers College of Business and Economics analyze data from forensic crime laboratories around the world to identify trends across laboratories and analyze individual laboratory performance. The project uses standardized definitions for a laboratory's functional areas and produces annual metrics to evaluate work processes, linking data on casework, personnel allocation, and financial information to work tasks and functions. Laboratory managers can then assess resource allocations, efficiencies, and value of services, with the goal of measuring a laboratory's operational data to identify and preserve what works and to change what does not. Although the Bureau of Justice Statistics (BJS)[1] and the National Institute of Justice (NIJ)[2; 3] approach forensic industry workloads and resources broadly, Project FORESIGHT highlights processes, strategies, resources, and allocations at a highly detailed level.

Participation in FORESIGHT is voluntary. Each participating laboratory receives a detailed analysis of its performance relative to all International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 17025 accredited laboratories in the project. A participating laboratory must submit its data using the project's Laboratory Reporting and Analysis Tool (LabRAT), a Microsoft Excel–based tool. LabRAT includes worksheets for minimum data submission (Level I) and, optionally, the submission of more detailed data in Level II. Level I data include the number of cases submitted in each area of investigation and the associated allocation of personnel across those areas. The corresponding financial data include the total salary and benefits in those investigative areas and the total laboratory expenditures for capital equipment and consumables and the total remaining expenditures. The optional Level II worksheets provide a more detailed report to each laboratory because they require the submission of additional detail on casework, personnel, and financials.

LabRAT

The LabRAT data collection tool is a workbook used to collect and automatically calculate business measures relating to caseloads, staffing, budgets, and other important factors. By itself, LabRAT is a useful tool for a laboratory manager, but submitting a completed LabRAT form allows West Virginia University to generate a benchmarking report for the submitting laboratory. Laboratories can use the LabRAT forms and FORESIGHT to evaluate their efficiencies and effectiveness better.

Common Definitions: One of FORESIGHT's strengths is its consistent use of specific terms, which are listed and defined in the Glossary. Following the terms and definitions as provided in the Glossary allows data submitted by various laboratories to be compared. "Turn-around time" is an excellent example of a term that varies in definition between laboratories and can only be compared when the Glossary definition is used. The founding FORESIGHT laboratories created the Glossary, which is updated periodically to ensure that the terms and definitions are current

with developing laboratory operations and technologies. Consistent definitions guide FORESIGHT participants to enter the correct data for benchmarking comparisons.

Investigative Areas: Although the structures of forensic laboratories vary around the globe, certain investigative areas are thematically consistent. The investigative areas used in FORESIGHT represent an attempt to capture this diversity while retaining accuracy about laboratory functions. Similar to the Glossary terms, FORESIGHT standardized definitions of investigative areas to help laboratories enter LabRAT data consistently.

FORESIGHT 2007–2020: Project FORESIGHT began in 2007, following a review of a similar project in Europe known as QUADRUPOL.[4] The initial Glossary terms and investigative area definitions followed those used in the QUADRUPOL project to facilitate comparison between North American and European laboratories. However, over time, FORESIGHT has updated its Glossary and investigative areas to generate statistical inferences for the North American experience. These updates have included expanding and collapsing investigative areas when the data represent too broad or too narrow a reflection, respectively, of laboratory functions.

II. Digital Evidence Casework and LabRAT Updates

Digital evidence casework is a FORESIGHT investigative area that was originally multiple investigative areas collapsed into one. The original 2007 LabRAT collection separated digital evidence into three areas: audio & video, speech & audio, and computer evidence.[a] Unfortunately, the sample size of laboratories reporting data on these three areas was too small to make any meaningful statistical inference. Subsequently, FORESIGHT data collection combined the three areas into a single digital evidence area that includes all computer, audio, and video digital analyses.

Digital evidence services are generally not located in the forensic crime laboratory, and agencies process evidence differently depending on the item of evidence. **Exhibit 1** shows the percentage of FORESIGHT laboratories that report processing digital evidence over time.

[a] The FORESIGHT glossary defines these categories: **Digital evidence** is the analysis of multimedia audio, video, and still image materials, such as surveillance recordings and video enhancement and includes computer analysis. **Computer analysis** is the analysis of computers, computerized consumer goods, and associated hardware for data retrieval and sourcing. **Speech & audio** is the analysis of live and recorded vocalizations in criminal investigations. These defined categories do not necessarily cover the full gamut of computer communications/metadata critical to digital evidence sets in certain cases or the cryptanalysis requirements fundamental to accessing such digital evidence.

Exhibit 1. Percentage of FORESIGHT laboratories reporting digital evidence analysis data

FY Ending	Accredited Laboratories Submitting FORESIGHT Data	Accredited Laboratories Reporting Digital Evidence Casework	Percentage of Accredited Laboratories with Digital Evidence Casework
2007	12	4	33
2008	9	1	11
2009	9	2	22
2010	20	2	10
2011	87	10	11
2012	86	7	8
2013	82	9	11
2014	152	28	18
2015	141	27	19
2016	145	32	22
2017	129	33	26
2018	151	35	23
2019	175	43	25
2020	163	47	29

Fiscal year (FY) 2018 was the first year that more than 30 laboratories reported casework in digital evidence analysis.[b] An inspection of the FORESIGHT data suggests there is a disparity among these laboratories with respect to the types of analyses conducted, with some metropolitan laboratories reporting very high caseloads and relatively low full time equivalent (FTE), whereas other laboratories report relatively low case volumes with much greater FTE per case. For all investigative areas, FORESIGHT follows the QUADRUPOL project's example and requests casework data on the numbers of cases submitted, items submitted, items outsourced, items examined internally, samples tested, tests performed, and reports issued. This disparity can be seen more clearly when examining the number of cases submitted, as shown by the FY2018 - FY2020 FORESIGHT data (**Exhibit 2**).

[b] **Exhibit 1** shows FY2016 and FY2017 with more than 30 digital evidence casework submissions. However, the submissions did not exceed 30 prior to the preparation of the annual report.

Exhibit 2. FORESIGHT laboratory cases submitted for Digital Evidence Analysis, FY2018

Case Submissions	Number of Laboratories in Range FY18	Number of Laboratories in Range FY19	Number of Laboratories in Range FY20
1–100	15	15	13
101–500	14	18	28
501–1,000	4	6	4
1,001–2,500	0	1	0
2,501–5,000	4	3	2

Given this disproportion , capturing data using the standard FORESIGHT measures is difficult because digital evidence is measured differently. Casework involving digital evidence can span from simple data extractions or automated processes to more advanced data analysis that requires specific types of forensic tools or training. Indeed, Project FORESIGHT's measures for casework often fail to capture the distinguishing features of digital evidence analysis, and thus, the collected data must be refined. This now includes digital forensic casework in general.

The Forensic Laboratory Needs Technology Working Group's (FLN-TWG) Digital Evidence subgroup led to some immediate changes to LabRAT. The disparity in caseload, where most laboratories reported fewer than 1,000 cases submitted while a few exceeded 2,500 cases annually, resulted in some immediate measurement changes for annual FORESIGHT reporting. The uniform casework collections in FORESIGHT request data on cases submitted, items submitted, items outsourced, items examined internally, samples examined, tests performed, and reports written, but the variety of digital evidence analytical requests offers poor comparable metrics for these casework details. As such, the FLN-TWG recommended that FORESIGHT update the uniform LabRAT data collection tool to collect information that might better represent a comparable metric. For FY2019, the ***volume of gigabytes (GB) examined*** was the simplest and most easily reported measure. The amount of data processed greatly affects the length of time needed to analyze it. For example, a 1 GB flash drive can be processed much faster than a 3 terabyte (TB) hard drive from a computer based on the volume of data needing to be processed. Counting the two items as equal is not accurate because the analysis time required for each may vary substantially. Examination of unallocated space to recover lost/deleted items versus a targeted examination of certain areas of data with known or suspected probative relevance will lead to variance in examination time.

The FORESIGHT LabRAT data collection tool asks the volume of GB examined in digital evidence in the Level II data request. Level II data are voluntary data beyond the minimum data submission requirement for analysis. As a new data request, submissions have been too low to

generate a general profile. Once FORESIGHT receives GB volume data submissions in sufficient numbers, the activity will be reported back to the FLN-TWG for reevaluation.

Given that much digital evidence casework is conducted outside the traditional forensic science laboratory, the FLN-TWG recommended that FORESIGHT create a second LabRAT tool to capture more detail on digital evidence casework. This second tool would be distributed to all laboratories reporting to the main LabRAT tool and to standalone digital evidence laboratories or units.

III. Identification of Digital Evidence Laboratories

To collect digital evidence casework data and corresponding business metrics, the FLN-TWG Digital Evidence subgroup compiled membership lists from the following agencies (see **Exhibits A-1** through **A-4**):

- ANSI-ASQ National Accreditation Board (ANAB) accredited laboratories
- American Association for Laboratory Accreditation (A2LA) accredited laboratories
- 2014 BJS Census of Publicly Funded Forensic Crime Laboratories Digital Evidence Pilot Study laboratories
- Internet Crimes Against Children (ICAC) Task Force Program state contacts

As the subgroup gathered these lists, they also made a more coordinated effort to capture all laboratories conducting digital evidence casework. Four members of the FLN-TWG Digital Evidence subgroup participated in an expert panel discussion with RTI International in its preparation for the next BJS Census of Publicly Funded Forensic Crime Laboratories. From the expert panel, it became clear that there are potentially over 10,000 agencies to contact for inquiries. Participants realized that gathering information regarding digital evidence casework was more extensive than initially imagined. Although the BJS Census grant award called for inclusion of all publicly funded forensic crime laboratories, the funding did not consider how many separate facilities were conducting digital evidence casework. Additionally, a laboratory conducting digital forensics may have similar tools and training as a specialized investigative unit targeting digital evidence, but the two entities are often not managed similarly. The 403 laboratories considered in the previous census could increase by many thousands if these additional digital forensics units are included, which the limited funding for the census grant did not consider. Therefore, efforts to extend Project FORESIGHT coverage to better collect data on digital evidence should be coordinated with the Census of Publicly Funded Forensic Crime Laboratories' digital evidence data collection (see **Section IV**).

Inquiries may begin through various organizations, such as the International Association of Chiefs of Police (IACP). Several organizations have provided training in digital evidence, including the National Computer Forensic Institute (NCFI), the National White Collar Crime Center (NW3C), the Federal Law Enforcement Training Center (FLETC), the Department of

Defense Cyber Crime Center (DC3), and the National Domestic Communications Assistance Center (NDCAC).

IV. Additional Data to Gather

In FY2019, collecting data on the volume of GB examined was a stop-gap attempt to gather some relevant details for digital evidence casework. Moving forward with a separate LabRAT data collection tool will require more detail, particularly for a standalone digital evidence laboratory or unit. Coordinating data collection with the BJS Census of Publicly Funded Forensic Crime Laboratories is recommended for consistency across time. Pilot studies with volunteer laboratories may be necessary to arrive at a useful data collection instrument.

Digital evidence analysts from the Houston Forensic Science Center met with the FLN-TWG Digital Evidence subgroup to offer suggestions on how to collect information relevant for FORESIGHT data analysis, which are listed below.

A. Consider breaking down categories similar to the original set of digital evidence categories in Project FORESIGHT. The Phoenix Police Laboratory has a breakdown that might serve as a basis, with digital evidence separated by type of device: mobile, computer, video, mass storage, and other (e.g., drones, watches, Internet of Things). The categorization should be flexible enough to account for rapid changes in technology (e.g., self-driving vehicles), and data capture should be flexible and forward thinking (e.g., vehicle analysis: software programs capture activity beyond GPS, doors opening and closing, hard braking, trunk opening, Bluetooth, and other devices).

B. Consider that within device type, it may be necessary to track number of items, data storage size of items, and time spent on various aspects of the analysis. For example, time spent on audio or video analysis is a more important workload metric than just the number of items examined. Audio files may be small but take much more time to analyze than an iPhone, which may have a large data storage size but does not take a lot of time to analyze using automated forensic tools. It is becoming useful to segregate the digital evidence source categories more granularly as these categories share common digital forensic workflow characteristics because of power, networking, expansion of memory, port availability versus direct access or disassembly of embedded systems, proprietary operating systems, and more.

C. Consider tracking time in detail. The Idaho State Police constructed a relatively simple system that could be adapted to break down amounts of digital evidence casework. Activity time tracking also permits greater detail on some of the unique challenges to the digital evidence workload, including technology review, casework, testimony, training time, continuing education, and attention to mental health issues (e.g., posttraumatic stress disorder risk from viewing child exploitation or violent content).

D. Coordinate data collection with other requests for data such as from IACP and the BJS Census of Publicly Funded Forensic Crime Laboratories. Consider the development of a

dashboard for digital evidence casework similar to that developed in FORESIGHT 20/20, where performance dashboards let management assess key metrics in real time. Digital forensic investigations occurring outside of a laboratory setting are increasing and must also be considered when possible.

E. Consider breaking down data by case type across digital evidence devices to identify trends and needs analysis.

F. Pay attention to Cloud storage issues. For example, consider what can and should be measured for storage capacity and if the measurement should be with respect to storage volume, storage cost, or some other consideration.

G. Consider more detailed personnel questions regarding sworn officers versus civilian analysts because career advancement pathways for sworn officers will pull them away from digital evidence casework, which can affect consistent returns over time.

As digital evidence is collected via the LabRAT tool, pay attention to key takeaways. The tool's development should be strategic and protect against short-sighted responses to changing needs. Additional concerns include the role of digital evidence units with response to data authentication, body camera evaluation, and maintaining public trust in laboratory objectivity and fairness.

V. Cost-Benefit Analysis

Digital evidence casework is expected to have a higher percentage of capital expenditures (e.g., personnel, capital, consumable, and overhead) relative to other areas of forensic science because of the breadth of evidence types and the associated costs for forensic tools needed to address the evolution in technology. Personnel expenditures are expected to include a greater amount of education and training costs for analysts to maintain proficiency with emerging technologies. FORESIGHT experience suggests that consumable expenditures and overhead account for a smaller percentage of total expenditures.

A. Estimated Cost of Instrumentation and Tools[c]

1. The costs associated with multiple tools should be considered. Several tools are typically needed for digital forensic casework, and technologies change more rapidly than in other areas of investigation. The following examples highlight some of the current tools that may lead to higher average annual expenditures for capital equipment:

    i. **Mobile Devices**: Graykey, Cellebrite, XRY, Magnet Axiom, Oxygen, Mobile Edit, Paraben, DataPilot

[c] Names of commercial manufacturers or products are incidental only. Inclusion does not imply endorsement by the authors or the U.S. Department of Justice.

ii. **Computer Forensics**: EnCase, FTK, X-Ways, Forensic Explorer, Blacklight, Sumuri Recon, Magnet Axiom

iii. **Forensic Audio/Video**: DVR Examiner, Avid, Ocean Systems, Cardinal, Final Cut, Photoshop

Each of these tools can cost over $10,000 initially with annual user license renewal expenditures each year (often in the $3,000–$4,000 range).

B. Cost of Evidence Retention and Storage

1. The increased internal capacity of computers and mobile and audio/video devices requires the collection of storage details that are not found in other areas of investigation. Data collection must consider local and Cloud storage expenses. Additionally, environments designed for cryptanalysis attacks on encrypted devices also bring design and custodial considerations and complexities.

C. Personnel Considerations

1. Training costs are considerably higher for digital evidence than other forensic sciences because of the rapid changes in technology. Training in this field is needed more frequently, and the costs and time required for training related to the recovery of digital evidence tend to be higher than other forensic science fields.
2. Digital evidence is processed largely in police department investigative units. Personnel in law enforcement environments are often faced with the following challenges:
    i. Lack of clear career progression (i.e., law enforcement vs. technical career path)
    ii. Unclear assignment of duties (i.e., splitting time between investigative and digital evidence duties)
    iii. Lack of defined role: forensic examiner or investigator
    iv. Resource utilization: Investment in training for an examiner who may be reassigned or promoted within a law enforcement department
3. A single examiner is capable of operating and managing multiple digital forensic processes simultaneously. Because personnel costs are generally higher than the cost of instrumentation/tools, this is a potential for cost savings.

D. Development Resources

1. The Forensic Technology Center of Excellence, through NIJ funding, will support the development of an updated data collection tool for FORESIGHT Digital Evidence Creation and Data Gathering.

E. Pros and Cons from Cost-Benefit Analysis of Digital Evidence Casework

1. Pros

i. The intelligence that can be gathered from digital evidence casework for investigative purposes is extremely valuable, including tracking a suspect's location, building timelines, and identifying behavior.

ii. In-house processing has a faster turn-around time versus outsourcing.

iii. Communicating directly with requestors to meet their needs versus sending to a third party.

iv. The ability to triage and reevaluate cases as investigators develop new leads allows them to focus investigations in a timely manner.

v. Wearables, mobile device data, and auto computing data are increasingly complementary for medical examiners and coroners, suggesting applicability across disciplines.

2. Cons

i. The diversity of the options and solutions for investigation and the rapid evolution of new technologies makes it difficult to standardize metrics across time for consistent managerial analysis. A simplified workflow (e.g., Collection and Preservation; Cryptanalysis/Access; Extractions; Analysis; Production) is recommended.

ii. Needing multiple tools necessary to provide accurate data for analysis can become expensive.

iii. Validation in this area is a challenge because of version control of software tools and patches.

3. Potential Resolution

i. Conduct a survey through the American Society of Crime Laboratory Directors on how members meet digital needs for investigative purposes.

ii. Seek input from training organizations with thousands of members like International Association of Computer Investigative Specialists, NW3C, FLETC, ICAC Task Force Program, Regional Computer Forensic Laboratories, U.S. Secret Service Electronic Crimes Task Forces, and others.

iii. Ask FLN-TWG members to identify how digital evidence needs are being met for investigative purposes.

F. Implications on Current Case Work and Return on Investment to Stakeholders (e.g., Law Enforcement, District Attorney's Office)

1. Gather additional FORESIGHT data.

2. Coordinate with the BJS Census of Publicly Funded Forensic Crime Laboratories.

VI. Implementation Plan Considerations

A. Outreach

1. Coordinate efforts with the Federal Bureau of Investigation (FBI) and Scientific Working Group on Digital Evidence for expert assistance in data collection tools.
2. Coordinate with the ICAC Task Force Program[5] administered by the Office of Juvenile Justice and Delinquency Prevention (OJJDP) under the Department of Justice's (DOJ's) Office of Justice Programs. Seek information from IACIS.com, LEVA.org, NW3C.org, and SEARCH.org. Also include the U.S. Secret Service NCFI (Hoover, AL) in coordination, outreach, and information gathering.
3. Coordinate with the Law Enforcement Cyber Center, which is funded by the Bureau of Justice Assistance and managed by the NW3C, the IACP, and the Police Executive Research Forum.
4. Reach out to accredited private laboratories (see Appendix).

B. Resources Needed

1. Identification of laboratories performing digital evidence casework—Coordinate with the BJS Census of Publicly Funded Forensic Crime Laboratories to maintain contact lists.
2. Identification of funding support to maintain and share collected data.

C. Challenges

1. Identification of agencies analyzing digital evidence. Currently, FORESIGHT only reports data from accredited laboratories in its comparison tables (even though FORESIGHT evaluates performance by accredited and non-accredited laboratories). Because there are so many non-accredited digital evidence laboratories and units, there may need to be dual reporting of the data to obtain a true sample of the work currently being performed.
2. Identification of data that should be collected in the FORESIGHT to determine what digital evidence metrics will be used to provide consistency in reporting.

D. Solutions

1. Begin to collect information on the volume of GB examined to supplement the caseload data with FY2019—Level II data in FORESIGHT.
2. Consider a separate data collection tool for Level II detail moving forward.
3. Communicate with commercial digital forensic tool manufacturers regarding customers and products (e.g., Cellebrite, EnCase, and FTK) to identify laboratories and agencies involved in processing digital evidence.

VII. Recommendations

A. Excerpts from NIJ's "Report to Congress for the Needs Assessment of Forensic Laboratories and Medical Examiner/Coroner Offices."[2]

– **Needs:**

- Resources and staffing to address the dramatic growth in digital and multimedia evidence (DME), now common for every case.
- Resources to purchase and maintain costly hardware and software tools and associated software licenses.
- Infrastructure for data storage of digital evidence to provide sufficient capacity and security to address operational requirements for data analysis and data sharing.
- Training for investigators and prosecutors to inform DME requests, increase understanding of the aspects of digital evidence, calibrate expectations, and produce meaningful DME results for developing investigative leads and for court cases.
- Dedicated personnel for DME casework and frequent training to stay current with new and emerging technologies.

– **Challenges:**

- Increased prevalence of encryption methods and encrypted devices and applications can impede DME investigations.
- DME examinations must continuously respond to new and emerging technologies and devices.
- DME functions may be carried out by personnel on a part-time or collateral duty basis, which can divert focus from the DME mission.
- Recruiting and retaining digital forensics experts is made more difficult as personnel are lost to retirement, promotions, private sector, burnout, or other factors.

– **Promising Practices:**

- Development of regional centers and task forces that provide resources and model infrastructure, such as the Regional Computer Forensics Laboratories administered by the FBI, U.S. Secret Service Electronic Crimes Task Forces, and the ICAC program administered by the U.S. DOJ's OJJDP.
- Education and training for investigators and prosecutors to identify DME data with potential investigative, probative, or forensic value.

- Introduction of triaging workflows across staff levels to examine and preserve evidence at the scene or early in the investigation, identify actionable information, facilitate real-time data analysis, maximize efficiencies, and help DME examiners prioritize casework.
- Dedicated DME personnel, salaries, benefits, and promotion opportunities commensurate with recruitment and retention of DME subject matter experts.
- Investments in DME tools for the examination of new and emerging digital technologies also responsive to evidentiary needs.
- Dedicated groups that perform software and tool testing and validation that can be shared with the DME community.
- Education and training to support implementation of quality management systems and accreditation efforts.

B. Education and training to support implementation of quality management systems and accreditation efforts. Develop and execute an education and training campaign that supports the implementation of quality management systems for laboratories seeking accreditation and for those that choose not to be accredited.

C. FORESIGHT data collection for digital forensics needs to be modified to more appropriately reflect the types of data that those laboratories collect. Digital laboratories do not log numbers of tests or number of samples. One suggestion is to collect the number of gigabytes processed rather than number of samples. Searching a 4 GB flash drive is much quicker than searching a 4 TB hard drive. The number of pieces of evidence may be of interest but the volume of data stored on each device is also important to measure.

D. Retrieving data from the Cloud is not solely a forensic process because it involves a legal element that must be considered. One technical issue is a determination of the legal authority for a forensic examiner to extract data from the Cloud. A typical search warrant for a cell phone does not authorize examiners to connect to the Cloud to download data that are not stored locally on a phone. Some extraction tools have the capability of using the keys/passwords stored on the phone to access data stored in the Cloud. However, in many jurisdictions, legal decisions contend that Cloud data exceeds the scope of the warrant because they are not stored locally. In fact, the data may be stored in another country outside of the United States.

E. The cost and accessibility of long-term data housing must be evaluated and supported, if warranted. The archival of large volumes of data is a technical concern of digital forensic laboratories. Some jurisdictions require evidence from certain crimes such as homicides to be retained indefinitely. The cost of storing these data is expensive and necessitates

discussions as to how this will be accomplished and how the evidence shall be stored (e.g., tape, Cloud based, additional network storage, external hard drives).

VIII. Validation Plan Considerations

A. Current FORESIGHT validation plan: Project FORESIGHT submissions undergo a search of publicly available data and reports to coordinate with data submissions in the first year of project participation. In subsequent years, changes in casework, personnel, and expenditures are compared with the prior validated submission. Inquiries are made with respect to all outliers, and only validated data are entered into the comparative metrics.

B. Accreditation issues: Although FORESIGHT provides all submitting laboratories an analysis, only accredited laboratories are included in the comparative database. The rapidly changing nature of technology and digital evidence casework makes this standard problematic. As such, the FLN-TWG recommended that FORESIGHT conduct a dual analysis of the data with two comparative groups: group 1 data from accredited laboratories or units and group 2 data from all submitting laboratories or units.

References

1. Bureau of Justice Statistics. "Data collection: census of publicly funded forensic crime laboratories." Washington, DC, U.S. Department of Justice, Office of Justice Programs. August 28. 2020. March 4 2022. Available from https://www.bjs.gov/index.cfm?ty=dcdetail&iid=244#:~:text=The%20Census%20of%20Publicly%20Funded%20Forensic%20Crime%20Laboratories%20(CPFFCL)%20is,organization%20is%20a%20government%20agency.

2. National Institute of Justice. 2019. *Status and needs of forensic science service providers: a report to congress*. Washington, DC: National Institute of Justice. Available from https://www.ncjrs.gov/pdffiles1/nij/213420.pdf.

3. National Institute of Justice. 2019. *Report to Congress: Needs assessment of forensic laboratories and medical examiner/coroner offices*. Washington, DC: National Institute of Justice. Available from https://www.ojp.gov/pdffiles1/nij/253626.pdf.

4. European Network of Forensic Science Institutes. 2003. *Quadrupol-development of a benchmarking model for forensic laboratories*.

5. OJJDP. "Internet Crimes Against Children Task Force Program." Washington, DC, Office of Juvenile Justice and Delinquency Prevention. n.d. Jul 18 2022. Available from https://ojjdp.ojp.gov/programs/internet-crimes-against-children-task-force-program.

6. ANSI National Accreditation Board (ANAB). "Directory of accredited organizations,"2022.

7. A2LA. "A2LA directory of accredited organizations." Frederick, MD, A2LA. n. d. March 4 2022. Available from https://customer.a2la.org/index.cfm?event=directory.index.

8. Bureau of Justice Statistics. 2018. Pilot Study of State and Federal Digital Evidence Laboratories, [United States], 2014: Inter-university Consortium for Political and Social Research.

9. Internet Crimes Against Children Task Force Program. "Task force contacts,"(n.d.).

Suggested Citation

NIJ Forensic Laboratory Needs Technology Working Group (FLN-TWG). (2022, August). *Implementation Strategies- Updating Data Collection for Digital Evidence Casework in Project FORESIGHT.* Forensic Technology Center of Excellence. U.S. Department of Justice, National Institute of Justice, Office of Investigative and Forensic Sciences.

Appendix Accredited Laboratories Listed by Accrediting Body

Exhibit A-1. ANSI ANAB Accredited Laboratories

ANAB Accredited
Alameda County Sheriff's Office Criminalistics Laboratory
American Express Digital & Multi-Media Forensic Laboratory
Anne Arundel County Police Department Forensic Services (Criminal Investigative Division/Digital Evidence)
Arkansas State Crime Laboratory (Little Rock Facility)
Baltimore County Police Department Forensic Services Section
Bureau of Forensic Science of Puerto Rico Criminalistics Laboratory
CACI, Inc. Digital Forensics Laboratory
California DOJ Fresno Laboratory
California DOJ Sacramento Laboratory
Charleston Police Department Forensic Services Division
Chicago Regional Computer Forensics Laboratory
Colorado Bureau of Investigation—Northern Colorado Regional Forensic Laboratory
Contra Costa County Office of the Sheriff Forensic Services Division (Summit Laboratory)
Cyber Security Malaysia Digital Forensics Laboratory
DC Department of Forensic Sciences
Defense Forensic Science Center
Denver Police Department
Department of Defense Cyber Crime Center—Cyber Forensics Laboratory
Drug Enforcement Administration (Chicago Sub-Regional Digital Evidence Laboratory)
Drug Enforcement Administration (Digital Evidence Laboratory)
Drug Enforcement Administration (Houston Sub-Regional Digital Evidence Laboratory)

ANAB Accredited
Drug Enforcement Administration (San Diego Sub-Regional Digital Evidence Laboratory)
Drug Enforcement Administration (Utah Sub-Regional Digital Evidence Laboratory)
FBI Digital Evidence Laboratory
Flashback Data, LLC
Florida Department of Law Enforcement Tallahassee Regional Crime Laboratory
Florida Department of Law Enforcement Tampa Bay Regional Crime Laboratory
Glendale Police Department—Verdugo Regional Crime Laboratory
Greater Houston Regional Computer Forensics Laboratory
Heart of America Regional Computer Forensics Laboratory
Houston Forensic Science Center
Intel Corporation—Global Forensics Investigations and eDiscovery (Folsom Campus)
Intel Corporation—Global Forensics Investigations and eDiscovery (Hawthorne Farms Campus)
Intel Corporation—Global Forensics Investigations and eDiscovery (Leixlip Campus)
Intel Corporation—Global Forensics Investigations and eDiscovery (Penang Campus)
Intermountain West Regional Computer Forensic Laboratory
Intermountain West Regional Computer Forensic Laboratory (Idaho Satellite Office)
Intermountain West Regional Computer Forensic Laboratory (Montana Satellite Office)
Johnson County Sheriff's Office Criminalistics Laboratory
Kansas Bureau of Investigation (Topeka Headquarters Laboratory)
Kentucky Regional Computer Forensics Laboratory
Mastercard Digital Forensic Laboratory
Minneapolis Police Department Crime Laboratory
Minnesota Bureau of Criminal Apprehension St. Paul Forensic Science Laboratory

ANAB Accredited
Montgomery County Police Crime Laboratory
National Digital Forensics Laboratory
New Hampshire State Police Forensic Laboratory
New Jersey Regional Computer Forensic Laboratory
New Mexico Regional Computer Forensics Laboratory
Nike Resilience Global Cyber Investigations Forensic Laboratory
North Carolina Department of Secretary of State Digital Forensic Laboratory
North Carolina State Crime Laboratory (Raleigh Laboratory)
North Texas Regional Computer Forensics Laboratory
Northwest Regional Computer Forensics Laboratory
Ohio Division of State Fire Marshal Forensic Laboratory
Oklahoma State Bureau of Investigation (AT&T Digital Forensics Laboratory)
Onondaga County Center for Forensic Sciences Laboratory
Orange County Regional Computer Forensics Laboratory
Philadelphia Regional Computer Forensics Laboratory
Procuraduría General de Justicia del Estado de Guanajuato—Agencia de Investigación Criminal—Laboratorio de Balística, Laboratorio de Documentos Cuestionados y Laboratorio de Informática Forense, Guanajuato
Ricoh Forensics
Rocky Mountain Regional Computer Forensics Laboratory
San Diego Police Department Forensic Science Section
San Diego Regional Computer Forensics Laboratory
San Diego Regional Computer Forensics Laboratory (Balboa Avenue)
Santa Clara County Office of the District Attorney Crime Laboratory

ANAB Accredited
Silicon Valley Regional Computer Forensics Laboratory
South Carolina Law Enforcement Division—Annex/Computer Crimes Center
Naval Information Warfare Systems Command—Systems Center Atlantic Cyber Forensics Criminal Investigations Laboratory
State of Connecticut Department of Emergency Services and Public Protection Division of Scientific Services
Target Forensic Services Laboratory (Las Vegas)
Target Forensic Services Laboratory (Minneapolis)
Texas Department of Public Safety Crime Laboratory Service—Austin Regional Crime Laboratory
Treasury Inspector General for Tax Administration Forensic and Digital Science Laboratory
Tucson Police Department Crime Laboratory
U.S. Customs and Border Protection Laboratories and Scientific Services—Los Angeles Laboratory
U.S. Customs and Border Protection Laboratories and Scientific Services—New York Laboratory
U.S. Customs and Border Protection Laboratories and Scientific Services—San Francisco Laboratory
U.S. Customs and Border Protection Laboratories and Scientific Services—San Juan Laboratory
U.S. Customs and Border Protection Laboratories and Scientific Services—Southwest Regional Science Center
U.S. Customs and Border Protection Laboratories and Scientific Services—Springfield Laboratory
U.S. Postal Service Forensic Laboratory Services
Virginia Department of Forensic Science Central Laboratory
Walmart eDiscovery & Forensic Services Laboratory
Westchester County Department of Laboratories and Research Division of Forensic Science

ANAB Accredited
Westchester County Department of Public Safety Crime Laboratory

Source: ANSI National Accreditation Board (ANAB)[6]

Exhibit A-2. A2LA Accredited Laboratories

A2LA Accredited
Ocean County Prosecutor's Office Digital Forensics Laboratory
Raleigh-Wake/City-County Bureau of Identification
U.S. Customs and Border Protection—Chicago Laboratory
U.S. Customs and Border Protection—Houston
U.S. Customs and Border Protection—Los Angeles Laboratory
U.S. Customs and Border Protection—New York Laboratory
U.S. Customs and Border Protection—San Francisco Laboratory
U.S. Customs and Border Protection—San Juan Laboratory

Source: A2LA[7]

Exhibit A-3. 2014 Census of Publicly Funded Forensic Crime Laboratories Digital Evidence Pilot Study

State	Agency Name	Laboratory Name
AK	Alaska Dept. of Public Safety	Technical Crimes Unit
AL	Alabama Dept. of Public Safety	Cyber Crimes Unit
AR	Arkansas State Crime Laboratory	Little Rock Laboratory (Headquarters)
AZ	Arizona Dept. of Public Safety	Computer Crimes Unit
CA	California Dept. of Justice	Fresno Regional Laboratory
CA	California Dept. of Justice	Jan Bashinski Laboratory
CA	California Dept. of Justice	Riverside Laboratory
CA	California Dept. of Justice	Sacramento Latent Print/Questioned Documents Laboratory
CA	U.S. Customs & Border Protection	San Francisco Laboratory
CA	U.S. DOJ—FBI	Regional Computer Lab—Orange County
CA	U.S. DOJ—FBI	Regional Computer Lab—San Diego
CA	U.S. DOJ—FBI	Regional Computer Lab—Silicon Valley
CO	U.S. DOJ—FBI	Regional Computer Lab—Rocky Mountain
CT	Connecticut Dept. of Public Safety	Forensic Science Laboratory
DC	Department of Veterans Affairs, Office of Inspector General	Computer Crimes and Forensics Laboratory
DC	Department of Homeland Security—Bureau of Customs & Border Protection	Laboratories & Scientific Services
DC	U.S. DOJ—Child Exploitation and Obscenity Section	High Technology Investigative Unit
DE	Delaware State Police	High Technology Crimes and Delaware Child Predator Task Force
FL	Florida Dept. of Law Enforcement	Tallahassee Regional Crime Laboratory
FL	Florida Dept. of Law Enforcement	Tampa Regional Crime Laboratory
GA	Georgia Bureau of Investigation	Child Exploitation and Computer Crimes Unit
GA	United States Army	Criminal Investigation Laboratory
HI	Hawaii Dept. of Public Safety/Dept. of Attorney General	Hawaii Internet and Technology Crimes Unit
IA	Iowa Dept. of Public Safety	Cyber Crime Unit
IL	Illinois State Police	Illinois DA High Tech Crimes Bureau
IL	Internal Revenue Service Criminal Investigation National Forensic Laboratory	National Forensic Laboratory
IL	U.S. DOJ—FBI	Regional Computer Lab—Chicago
IN	Indiana State Police	Cyber Crime Unit
KS	Kansas Bureau of Investigation	High Technology Crime Unit
KS	Kansas Bureau of Investigation	Topeka Laboratory
KY	Kentucky Office of the Attorney General	Cyber Crimes Unit

State	Agency Name	Laboratory Name
KY	Kentucky State Police	Technical Services Division, Electronic Crimes Branch
KY	U.S. DOJ—FBI	Regional Computer Lab—Kentucky
LA	Louisiana State Police	Technical Support Unit
MD	Department of Defense	Cyber Crime/Computer Forensics Center
MD	Maryland State Police	Computer Forensics Lab
MD	Treasury Inspector General for Tax Administration	Forensic Science Laboratory
ME	Maine State Police	Computer Crimes Unit
MI	Michigan State Police	Computer Crimes Section—Computer Crimes Unit
MN	Minnesota Bureau of Criminal Apprehension	Minnesota ICAC Task Force
MO	Missouri State Highway Patrol	Digital Forensics Investigative Unit
MO	U.S. DOJ—FBI	Regional Computer Lab—Heart of America
MS	Mississippi Office of the Attorney General	Cyber Crime Unit
MT	Montana DOJ Highway Patrol	Computer Crime Section
NC	North Carolina State Bureau of Investigation	Computer Crimes Unit
NC	North Carolina State Bureau of Investigation	Raleigh Crime Laboratory
NE	Nebraska State Patrol	Computer Forensics Lab
NH	New Hampshire State Police	Forensic Laboratory
NJ	New Jersey State Police	Computer Crimes and High Technology Surveillance Bureau
NJ	U.S. DOJ—FBI	Regional Computer Lab—New Jersey
NM	U.S. DOJ—FBI	Regional Computer Lab—New Mexico
NY	New York Division of State Police	Computer Forensic Laboratory
NY	U.S. DOJ—FBI	Regional Computer Lab—Western NY
OH	Ohio State Fire Marshal	Forensic Laboratory
OH	Ohio State Patrol	Computer Crimes Unit
OH	U.S. DOJ—FBI	Regional Computer Lab—Miami Valley
OK	Oklahoma State Bureau of Investigation	Computer Crimes Unit
OR	Oregon State Police	Major Crimes Section
OR	U.S. DOJ—FBI	Regional Computer Lab—Northwest
PA	Pennsylvania State Police	Computer Crime Unit
PA	U.S. DOJ—FBI	Regional Computer Lab—Philadelphia
RI	Rhode Island State Police	Computer Forensic Laboratory
SC	South Carolina Law Enforcement Division	Computer Crimes Center
SC	South Carolina Law Enforcement Division	Forensic Laboratory

State	Agency Name	Laboratory Name
TN	Tennessee Bureau of Investigation	Technical Services Unit
TX	Texas Attorney General's Office	Computer Forensics Unit
TX	Texas Dept of Public Safety	Austin Laboratory
TX	U.S. DOJ—FBI	Regional Computer Lab—Greater Houston
TX	U.S. DOJ—FBI	Regional Computer Lab—North Texas
UT	U.S. DOJ—FBI	Regional Computer Lab—Intermountain West
VA	Department of Homeland Security	Bureau of Immigration and Customs Enforcement
VA	Department of Homeland Security	Homeland Security Investigations
VA	Drug Enforcement Administration	Digital Evidence Laboratory
VA	FBI	Crime Laboratory
VA	Naval Criminal Investigative Services	Headquarters (Quantico)
VA	U.S. DOJ—FBI	Computer Analysis Response Team
VA	U.S. DOJ—FBI	Digital Evidence Lab
VA	U.S. Postal Inspection Service	Forensic Laboratory Services
VA	Virginia Dept of Forensic Science	Central Laboratory
VA	Virginia State Police	Computer Evidence Recovery Section
VT	Vermont State Police	Computer Crimes Unit
WA	Washington State Patrol	High Tech Crime Unit
WI	Wisconsin Dept of Justice	Division of Criminal Investigation
WI	Wisconsin State Crime Laboratory	Milwaukee Laboratory
WI	Wisconsin State Crime Laboratory	Wausau Laboratory
WV	West Virginia State Police	Digital Forensics Laboratory
WY	Wyoming Office of the Attorney General	Computer and High-Tech Crime Center

Source: Bureau of Justice Statistics[8]

Note that only state and federal laboratories were included in the pilot study. No county/municipal laboratories were evaluated.

Exhibit A-4. ICAC State Contacts

State	Agency
Alabama	Alabama Law Enforcement Agency
Alaska	Anchorage Police Department
Arizona	Phoenix Police Department
Arkansas	Arkansas State Police
California—Fresno Area	Fresno County Sheriff's Office
California—Los Angeles Area	Los Angeles Police Department
California—Sacramento Area	Sacramento County Sheriff's Office
California—San Diego Area	San Diego Police Department
California—San Jose Area	San Jose Police Department
Colorado	Colorado Springs Police Department
Connecticut	Connecticut State Police
Delaware	Delaware DOJ
Florida—Central	Osceola County Sheriff's Office
Florida—Northern	Gainesville Police Department
Florida—Southern	Broward County Sheriff's Office
Georgia	Georgia Bureau of Investigation
Hawaii	Hawaii Department of Attorney General
Idaho	Idaho Office of Attorney General
Illinois	Illinois Office of Attorney General
Illinois—Cook County Area	Cook County State's Attorney's Office
Indiana	Indiana State Police
Iowa	Iowa Division of Criminal Investigation
Kansas	Sedgwick County Sheriff's Office
Kentucky	Kentucky State Police
Louisiana	Louisiana DOJ
Maine	Maine State Police
Maryland	Maryland State Police
Massachusetts	Massachusetts State Police
Michigan	Michigan State Police
Minnesota	Minnesota Bureau of Criminal Apprehension
Mississippi	Mississippi Office of Attorney General
Missouri	St. Charles County Police Department
Montana	Montana Division of Criminal Investigation
Nebraska	Nebraska State Patrol
Nevada	Las Vegas Metropolitan Police Department
New Hampshire	Portsmouth Police Department
New Jersey	New Jersey State Police
New Mexico	New Mexico Office of the Attorney General

State	Agency
New York	New York State Police
New York—New York City Area	New York City Police Department
North Carolina	North Carolina State Bureau of Investigation
North Dakota	North Dakota Bureau of Criminal Investigation
Ohio	Cuyahoga County Prosecutor's Office
Oklahoma	Oklahoma State Bureau of Investigation
Oregon	Oregon DOJ
Pennsylvania	Delaware County District Attorney's Office
Rhode Island	Rhode Island State Police
South Carolina	South Carolina Attorney General's Office
South Dakota	South Dakota Division of Criminal Investigation
Tennessee	Knoxville Police Department
Texas	Office of the Attorney General of Texas
Texas	Dallas Police Department
Texas—Houston Area	Houston Police Department (Houston Metropolitan)
Utah	Utah Office of Attorney General
Vermont	Vermont Office of the Attorney General
Virginia—Bedford County Area	Bedford County Sheriff's Office
Virginia	Virginia State Police
Washington	Seattle Police Department
West Virginia	West Virginia State Police
Wisconsin	Wisconsin DOJ
Wyoming	Wyoming Division of Criminal Investigation

Source: ICAC Task Force Program [9]

Forensic Technology
CENTER OF EXCELLENCE
A program of the National Institute of Justice

NIJ | National Institute of Justice
STRENGTHEN SCIENCE. ADVANCE JUSTICE.

NIJ is dedicated to improving knowledge and understanding of crime and justice issues through science. NIJ provides objective and independent knowledge and tools to inform the decision-making of the criminal and juvenile justice communities to reduce crime and advance justice, particularly at the state and local levels. The NIJ Office of Investigative and Forensic Sciences (OIFS) is the federal government's lead agency for forensic science research and development. OIFS's mission is to improve the quality and practice of forensic science through innovative solutions that support research and development, testing and evaluation, technology, information exchange, and the development of training resources for the criminal justice community.