National Case Closed Project:

Guidance on the Application of Digital Evidence in Shooting Investigations

Summary and Purpose

The National Case Closed Project (NCCP), a Bureau of Justice Assistance initiative coordinated by RTI International, supports law enforcement agencies nationwide in improving their violent crime clearance rates, especially for fatal and nonfatal shootings. RTI provides customized training and technical assistance to these agencies based on an assessment of current challenges and available resources to support them in improving their response to shootings.

Law enforcement agencies and laboratory partners often deal with extreme limitations when it comes to digital evidence (DE) processing, analysis, and viability in court. This can be especially challenging for agencies with limited resources that are facing issues such as funding restrictions, low staffing, and a lack of specialized training. The purpose of this NCCP brief is to inform law enforcement agencies of the critical role that DE plays in supporting investigations, to describe promising practices from the field, and to provide resources that can benefit agencies including standards and recommended guidelines.

Importance of Digital Evidence

DE is used in investigations to support and corroborate other types of evidence. Having access to a digital "footprint" of victims, suspects, or even witnesses encourages a more comprehensive approach to any investigation. According to the Digital Evidence Policy and Procedures Manual developed by the National Institute of Justice in 2020, DE is defined as "information stored or transmitted in binary form that may be relied on in court … and can be found on a computer hard drive, a mobile phone, among other places" (National Institute of Justice, 2020). Common sources of DE in shooting investigations include cell phone tower location data, camera video footage, vehicle location data, and messages and other data extracted from cell phones and social media activity.

How DE Supports Investigations of Fatal and Nonfatal Shootings

The use of DE in criminal proceedings has increased significantly in recent years, as law enforcement obtains location services, online activity, and much more to seek leads in locating suspects, providing key breaks in investigations, or securing case adjudication. With respect to shooting investigations, DE can be accessed on mobile devices such as cell phones or laptops to understand the specific movements or whereabouts of subjects. It can also be useful for confirming the involvement—or lack thereof—of certain individuals or incidents through call/text activity or social media presence. Proactive investigative tools such as video surveillance (e.g., body cameras, dash cameras, closed-circuit television [CCTV]), license plate readers, or GPS devices also positively impact agencies' investigative outcomes.

This NCCP brief provides information on national-level organizations that support the development of best practices, guidelines, and application-specific resources that can be helpful to law enforcement leadership. Selected resources are highlighted, which may provide information on adopting policies or application-specific strategies.

Developing and implementing effective procedures for collecting, storing, and analyzing DE can be challenging, especially given resource constraints (e.g., funding, staffing) and competing priorities. However, the installation or optimization of specific DE practices and tools will not only support case resolutions but can also supplement other investigative practices already being implemented, and thus should be a priority for law enforcement leaders. To support agencies in enhancing their use of DE in shooting investigations, the following highlights innovative practices and organizational changes that law enforcement agencies have implemented to improve their utilization of DE for investigations.

Albuquerque Police Department Agency Spotlight—Digital Intelligence Team

In 2021, the Albuquerque Police Department (APD) introduced its Digital Intelligence Team (DIT). Historically, DE analysis within the department had been fragmented, with detectives who were inconsistently trained trying to manage the process alongside other duties. With the establishment of the DIT, APD was able to reduce turnaround times and, in turn, improve its case clearance rates and investigative outcomes. In particular, APD has prioritized the analysis of available DE for all homicide cases with the DIT also assisting many other types of cases including sexual assault and nonfatal shootings. During the first 12 months of DIT's full-time involvement in homicide cases, APD reported a doubling (from 42% to 85%) in its homicide clearance rate, with most of those cases using DE to help strengthen the cases.

Important features of the DIT are the types of staff used, the application of a full-time unit supervisor, and the development of clear lines of connection between the DIT and criminal investigators. The DIT is comprised entirely of non-sworn professionals, which helps protect the team from dividing up daily job duties in other areas within the APD and promotes sustainability. The staffing structure includes 2 supervisors, 10 forensic examiners, and 2 evidence-handling technicians. DIT staff collaborate with lead detectives on cases and participate in regular accountability meetings with investigators to review case decisions to ensure that no critical DE is overlooked. To further support this collaboration, coordination with the DIT team to collect and analyze DE is included in the APD shooting checklist.

Supervisors are responsible for overseeing the entire process to ensure balanced caseloads and quality performance, and for ensuring that tasks such as software updates and license renewals are completed. Given its growth and demand, the DIT now requires a dedicated full-time supervisor to manage day-to-day operations. A dedicated supervisor can support ongoing education of sworn personnel on the importance of DE, particularly since buy-in and awareness are key toward achieving consistent utilization across cases.

Forensic Examiners conduct phone extractions and other types of DE processing, craft expert-level reports, attend accountability meetings, and provide court testimony as needed.

Technicians are responsible largely for assisting with device extraction, along with cloud uploading of data for examiners or detectives and providing administrative support.

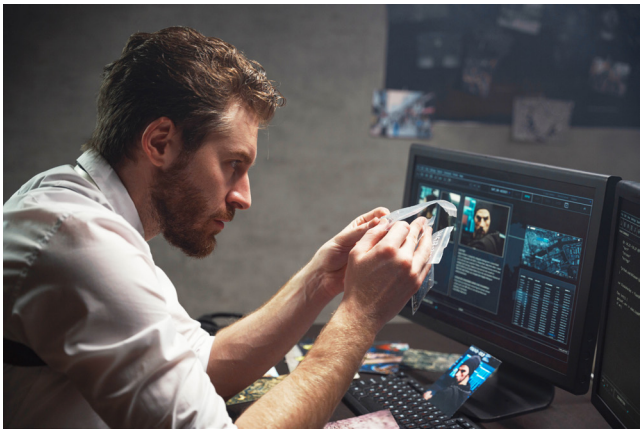
Looking ahead, APD has identified video surveillance analysis as another area to address, particularly the need for increased analysis capacity and video footage enhancement. Creating a specialized team to focus on video analysis, similar to the DIT, is currently being considered.

Highlights from NCCP Site Assessments

The NCCP assessment process has identified the different needs and approaches that agencies are taking to strengthen how they utilized DE for fatal and nonfatal shooting investigations, including advancements in policy and training. Examples include the areas that follow.

Policy Advancement: The Greensboro Police Department (GPD) has updated its policies and procedures for requesting, processing, documenting, and analyzing DE through its *Digital Forensics Lab Procedure SOP*. These updates have enhanced the roles and responsibilities of GPD's DE staff while also promoting continuity when there is turnover within the DE unit as well as long-term adaptability and sustainability. Although only two members of the GPD Digital Forensics Lab are currently processing devices, they are completing up to 75 analyses per month. To support and potentially increase this level of processing, GPD is exploring additional training opportunities and certifications for DE staff. GPD Digital Forensics Lab policies are also supplemented with process flow charts and training materials to promote consistency in engaging DE staff in investigative processes. DE staff routinely provides training to investigative staff as well as GPD's training academy to support consistency in DE utilization.

Training Curriculum: Because of identified gaps in DE collection versus DE processing, the Lansing Police Department (LPD) was urged to seek additional training and support in relevant DE topic areas, including social media and video evidence. To support these recommendations, LPD is updating department policies and processes as they relate to the utilization, documentation, and analysis of DE in cases. To support these efforts, LPD is exploring additional training for staff in DE collection and analysis to include the use of social media in investigations. LPD also uses crime analysts to strengthen the department's capacity in video evidence analysis. Recommendations were also expanded to include the Ingham County Prosecuting Attorney's Office to support the collaboration and effective usage of DE for case prosecution.



Staff Roles & Responsibilities: The Salt Lake City Police Department (SLCPD) has taken a comprehensive approach with DE processing. The seizure, extraction, and analysis of DE is performed by a variety of units, including patrol officers, crime scene investigators, detectives, and crime analysts. Although this highlights the versatility of personnel to handle these demands, it could lead to inconsistent practices or even duplicated efforts. SLCPD was encouraged to leverage its crime analysts more and provide clarity by assigning processing tasks more consistently to ensure a streamlined workflow. To align with these recommendations, SLCPD is updating department policies, procedures, and checklists to provide additional clarity on investigative roles and responsibilities as they relate to DE. To reinforce these policies, SLCPD developed in-house investigator training academies, which are open to all officers and investigators. The department has also reallocated department staff to perform DE analysis while also creating a new position that specifically supports video evidence collection and analysis. As SLCPD builds out its DE capacity, the department hopes to add additional DE staff and integrate this into its developing Real Time Crime Center.

Recommendations for Implementing a DE Unit

For agencies considering the development of a standalone unit for analyzing DE, the NCCP team compiled a set of recommendations to support the process. An independent DE unit can optimize an agency's procedures by reducing turnaround times, streamlining communication workflows, and providing clarity regarding the responsibilities of personnel.

1. Develop written policies and procedures for collecting, processing, and storing DE.
2. Assign dedicated personnel to analyze DE to increase efficiencies and decrease processing turnaround times. Consider assigning or onboarding non-sworn personnel to support in this area.
3. Install a "laboratory liaison" position to bolster communication efforts, streamline procedures, and support consistent messaging.
4. Enable DE-specific evidence tracking mechanisms to support storage and security of large amounts of data.
5. Develop training plans for analysts working with DE to optimize workflows, increase processing capabilities, and maintain up-to-date standards and best practices.
6. Draft a report writing template for use among analysts and law enforcement agencies to support consistency across casework.
7. Include DE staff and supervisors in regular accountability meetings with investigators to simplify communication and evidentiary priorities.
8. Assess available resources that can be allocated for DE-specific responsibilities. Consider applying for federal grant funding to support this effort.
9. Explore partnering with federal law enforcement organizations or task forces to leverage more expensive equipment. Similarly, share DE resources with other local agencies (e.g., space, training, equipment, software), including prosecutors, to achieve cost savings.
10. Use other law enforcement agencies' successes as a model. For more information, see "Albuquerque Police Department Agency Spotlight—Digital Intelligence Team."

National Scientific Organizations

National organizations that support and emphasize the use of DE include scientific organizations that have produced standards, guidelines, and best practices to help inform and educate practitioners. These organizations and their corresponding resources are beneficial for law enforcement to access and understand for use in their own agencies.

The Organization of Scientific Area Committees for Forensic Science (OSAC)—Digital Evidence Subcommittee

The OSAC Digital Evidence Subcommittee collaborates with experts nationwide to produce and support **standards and guidelines** that are considered of "probative value" and relevant for forensic science applications. These standards and guidelines help frame the appropriate and effective use of DE for investigative purposes.

For more information, visit Organization of Scientific Area Committees for Forensic Science Digital Evidence Subcommittee

Selected resources from the OSAC DE subcommittee include the following:

- Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics (guidance document)
  - Document, developed through the Scientific Working Group on Digital Evidence and published by the OSAC Digital Evidence Subcommittee, includes recommendations for testing core tools that support forensic examinations. It outlines minimum requirements for verification testing of forensic tools that will set up department laboratories for success.
- Standard Terminology for Digital and Multimedia Evidence Examination* (standards document)
  - International standard includes terminology and definitions used in the field of digital forensics to ensure effective use and reference among practitioners.
- Standard Guide for Forensic Audio Laboratory Setup and Maintenance* (standards document)
  - Guide overviews the standard practice for outfitting an agency with the necessary equipment and space to optimize the analysis of forensic audio.

For a full list of standards and other resource materials developed, please visit the webpage here: Organization of Scientific Area Committees for Forensic Science Digital Evidence Subcommittee Standards

*** Requires the creation of an online account to access.**

Scientific Working Group on Digital Evidence (SWGDE)

SWGDE is a formal working group founded to develop and promote **best practices** for DE applications in a forensic-related manner. The resources produced by the SWGDE aim to provide a quality assurance framework for field use. SWGDE is divided into six main committees, distinguished by DE focus areas, such as forensics, audio, imaging, photography, video, and quality and standards.

For more information, visit Scientific Working Group on Digital Evidence

Selected resources from the SWGDE include the following:

- Core Competencies for Digital Forensics – DRAFT 7.3.2024 (guidance document)
  - This draft list of core competencies provides insight on the various categories of expertise that forensic examiners should possess. Specific areas outlined in this document include but are not limited to legal considerations and ethical standards, search and identification, data acquisition, documentation, and presentation and testimony.
- SWGDE Guidelines & Recommendations for Training in Digital & Multimedia Evidence (recommendations guide)
  - It's important to understand the necessary training components for all staff that encounter DE as part of an investigation. This guide lays out considerations for ensuring that personnel are educated on and equipped with the necessary resources to effectively use DE in a given case.
- SWGDE Best Practices for Digital Forensic Video Analysis (recommendations guide)
  - Analyzing video evidence can be challenging but is a crucial step and can shift an investigation. These recommendations were published to provide a framework for processing video evidence and successfully introducing it in court.
- SWGDE Best Practices for Obtaining Google Reverse Location Data for Investigative Purposes (recommendations guide)
  - Geographical mapping is a critical component of many investigations. This recommendation guide provides best practices for obtaining data from Google as supporting evidence.

SWGDE has published a variety of materials, with an increased frequency since 2022. They are available here: Scientific Working Group on Digital Evidence Published-By Committee

Other Resources

Other available resources include publications describing the selected applications of DE, including artificial intelligence (AI) and its benefit to investigations, search and seizure best practices, a policy and procedures manual, and considerations for the processing and analysis of DE. These resources are intended to inform readers of the benefit to specific applications that exist but also to provide a framework for using them effectively and within the limitations of a given agency.

Attaway, P., Williams, C., Daye, C., Bynum, N., Weinstein, L., and Johnson, R. (2023).*The new DNA: Recommendations for agencies to consider implementing to improve digital evidence processing and analysis.* Submitted to the National Institute of Justice. https://forensicrti.org/wp-content/uploads/2023/12/Digital-Evidence-In-Brief_FINAL.pdf

- This research, funded by the National Institute of Justice, provides findings from a quantitative survey and qualitative interviews of both law enforcement and crime laboratory staff; it also includes considerations for DE processing and analysis that may assist in understanding limitations and best practices for agencies in the United States.

Federal Law Enforcement Training Centers (FLETC). (2024). Training catalog. https://www.fletc.gov/training-catalog?combine=digital+evidence&field_locations_offered_value=All

- A variety of training opportunities are available through the FLETC, depending on your affiliation. Some federal agencies are considered partners and are eligible for training, while others can easily apply for training. Courses are available from a beginner to intermediate level on digital forensics examination, evidence acquisition, mobile device techniques, operating system considerations, and data recovery.

Criminal Justice Testing and Evaluation Consortium. (2020). *Artificial intelligence applications in law enforcement.* https://cjtec.org/files/65532c5cad011

- Targeting law enforcement executives, this brief discusses law enforcement applications for AI. It specifically focuses on defining AI, understanding law enforcement use cases, and providing current and emerging applications.

Interpol. (2021). *Guidelines for digital forensics first responders: Best practices for search and seizure of electronic and digital evidence.* https://forensicresources.org/resources/guidelines-for-digital-forensics-first-responders/

- This guidance document, which targets law enforcement and first responders, provides guidance and structured strategies for DE collection on-scene. Technical considerations and application-specific guidance procedures are also included in this informative brief.

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

- This robust reference manual provides law enforcement with a foundation for developing policies and procedures for collecting, handling, and processing DE. This resource also assists laboratories in performing the DE accreditation process.

National White Collar Crime Center (NW3C). (2024). *Course catalog.* https://www.nw3c.org/UI/CourseCatalog.html

- This catalog provides a list of robust set of no-cost trainings that are available through the NW3C for criminal justice practitioners, including many on digital forensics. Topics include basic digital forensic analysis, seizure, automated forensic tools, encryption, and software-specific content (e.g., Windows, MacOS, iOS, Android).

Forensic Technology Center of Excellence. (2022). *Digital caseload processing with the NIST National Software Reference Library.* https://forensiccoe.org/webinar-2022-software-reference-library/

- This webinar, hosted in 2022, discusses the National Software Reference Library (NSRL) and National Institute of Standards and Technology (NIST) and how they support efficient and effective use of computer technology in investigations. Changes to the NIST NSRL may affect the application of certain digital forensic tools.

Forensic Technology Center of Excellence. (2022). *Audio forensic analysis procedures for user generated audio recordings.* https://forensiccoe.org/webinar-2022-audio-forensic-analysis/

- This webinar, hosted in 2022, discusses the use of devices capable of recording audio/video and the best way to combine the information available from these recordings for use in forensic analysis and investigations.

Forensic Technology Center of Excellence. (2021). *Best practices for digital image processing.* https://forensiccoe.org/best-practices-image-processing/

- This webinar, hosted in 2022, discusses the art of digital imaging and expands the knowledge of attendees through applying processing techniques for use in criminal justice proceedings.

More Information

If you have questions or want more information on the National Case Closed Project, please contact us.

NCCP Helpdesk

NCCP Website

This project is supported by Grant No. 15PBJA-21-GK-04008-JAGP awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance (BJA) is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.