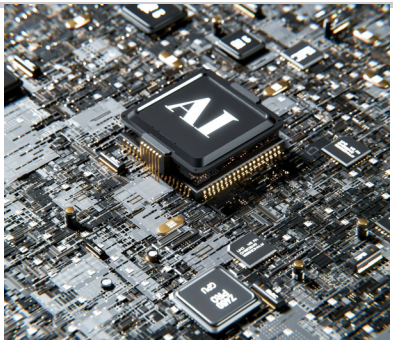
Navigating the digital deluge: Preparing for the future of evidence

The plethora of digital evidence available to law enforcement is bringing actionable insights to investigations and strengthening cases for prosecution, but it must be managed with care

By Chief Philip Lukens, Ret.

Reprinted with permission from Police1.com

The explosion of digital evidence from multiple sources



Law enforcement agencies are facing a staffing crisis due to a decline in applications and an increase in resignations and retirements. One of the ways to cope with this challenge is to leverage technology, such as automated license plate recognition (ALPR) systems, body cameras, drones and community sources, to augment capabilities of sworn officers. These technologies can generate a vast amount of digital evidence that can help law enforcement agencies to locate and apprehend suspects, prevent or solve crimes and recover stolen property. ALPR systems, for instance, are computer-controlled camera systems that can capture and analyze license plate images from vehicles and compare them to databases of vehicles of interest. ALPR systems can also access archived data from real time crime center (RTCC) databases to provide insights for investigators on cold cases.

However, digital evidence is not only useful for law enforcement, but also for prosecution. By providing accurate and reliable evidence of the location, movement and association of vehicles and suspects, as well as video, audio and biometric data, digital evidence can help prosecutors to build strong cases, corroborate witness statements and refute defense claims. Digital evidence can also help prosecutors to identify patterns of criminal activity, link multiple cases and establish criminal intent and motive. Furthermore, digital evidence can help prosecutors to streamline the discovery process, reduce the need for plea bargains and increase the conviction rate.

The challenges of managing and analyzing unstructured data

While digital evidence can be a powerful tool for law enforcement and prosecution, it can also pose some challenges in terms of data management and analysis. Digital evidence is voluminous, complex and dynamic, requiring a lot of storage space, processing power and analysis skills. Moreover, digital evidence is often unstructured, meaning that it does not have a predefined format or schema, such as text, images, audio or video. Unstructured data is difficult to organize, search, and interpret, as it may contain noise, ambiguity or inconsistency. Furthermore, unstructured data is subject to various legal and ethical standards, such as privacy, transparency and accountability, which require proper policies, procedures and safeguards to ensure compliance.

Therefore, law enforcement agencies need a system that not only collects digital evidence, but also processes it into actionable insights, which is crucial for effective law enforcement and case resolution. Such a system should be able to filter, organize and analyze the unstructured data, as well as generate reports, alerts and recommendations. Moreover, such a system should be able to protect the data from unauthorized access, modification and deletion, as well as encrypt, backup and audit the data. Furthermore, such a system should be able to integrate the data with other sources, such as video, audio and biometric data, to provide a comprehensive picture of the situation.

Best practices for preparing law enforcement and prosecutors for digital evidence

One of the best practices for preparing law enforcement and prosecutors for digital evidence is to provide them with adequate training and education on the technical, legal and ethical aspects of regulations for accessing, sharing and disclosing digital evidence. Moreover, they need to understand the ethical and social implications of using digital evidence, such as the impact on privacy, civil rights and public trust.

Another best practice for preparing law enforcement and prosecutors for digital evidence is to provide them with adequate resources and support for managing and analyzing digital evidence. Law enforcement and prosecutors need to have access to sufficient storage space, processing power and analysis tools for handling digital evidence. Furthermore, they need to have access to reliable and secure networks, systems and platforms for communicating and collaborating with digital evidence.

The importance of AI-enabled image and data analysis in surfacing key evidence

One of the ways to enhance the processing and analysis of digital evidence is to employ artificial intelligence (AI) techniques, such as machine learning, computer vision and natural language processing, to enhance the image and data analysis capabilities of the system. AI can help to automate the verification and classification of the unstructured data, as well as to

Continued on next page

Continued from previous page

detect anomalies, patterns and relationships among the data. AI can also help to extract relevant and meaningful information from the data, such as faces, objects, emotions and sentiments. AI can also help to generate summaries, visualizations, and narratives from the data, as well as to provide suggestions, predictions and explanations based on the data.

However, AI also poses some challenges and limitations in terms of data quality, bias, transparency and accountability. AI relies on the data that is fed into it, which may be incomplete, inaccurate, possess blind spots or be outdated. AI may also reflect the biases and assumptions of the data or the algorithms, which may lead to unfair or inaccurate outcomes. AI may also be difficult to understand or explain, especially for complex or sensitive decisions, which may raise ethical and legal questions. AI may also be subject to errors, failures, or attacks, which may affect its performance and reliability.

Therefore, law enforcement agencies need to ensure that the AI-enabled image and data analysis system is robust, reliable and responsible, as well as aligned with the legal and ethical standards of using digital evidence. Law enforcement agencies need to validate and monitor the data and the algorithms, as well as to mitigate and correct any biases or errors. Law enforcement agencies also need to ensure that the system is transparent and explainable, as well as to document and justify the decisions and actions based on the system. Furthermore, law enforcement agencies need to secure and audit the system, as well as to report and respond to any incidents or issues.

Strategies for ensuring that digital evidence strengthens the prosecutorial process

One of the strategies for ensuring that digital evidence strengthens the prosecutorial process is to establish a close and effective collaboration between law enforcement and prosecution, as well as between civilian data analysts and sworn officers. Law enforcement and prosecution need to communicate and coordinate with each other on the collection, preservation, and presentation of digital evidence, as well as on the legal and ethical issues that may arise from using digital evidence. Civilian data analysts and sworn officers need to communicate and coordinate with each other on the verification, analysis, and interpretation of digital evidence, as well as on the technical and operational issues that may arise from using digital evidence. Moreover, law enforcement, prosecution, and civilian data analysts need to foster a culture of trust, respect, and cooperation, as well as to share best practices and lessons learned from using digital evidence.

Another strategy for ensuring that digital evidence strengthens the prosecutorial process is to adopt a proactive and innovative approach to using digital evidence, as well as to leverage the opportunities and benefits that digital evidence offers. Law enforcement and prosecution need to seek and exploit the potential of digital evidence to enhance their investigations and prosecutions, as well as to anticipate and address the challenges and risks that digital evidence poses. Law enforcement and prosecution also need to explore and experiment with new and emerging technologies and techniques that can generate, process, and analyze digital evidence, as well as to evaluate and validate their effectiveness and efficiency. Furthermore, law enforcement and prosecution need to engage and educate the public and the stakeholders on the value and impact of digital evidence, as well as to solicit and incorporate their feedback and input.

The need for software to provide a summary for prosecution in a readable and presentable format

One of the challenges that law enforcement and prosecution face when using digital evidence is to provide a summary of the evidence in a format that is readable, understandable and able to be presented in court effectively. Too much uncategorized data can end up having no value, as it can overwhelm, confuse or mislead the prosecutors, the judges and the jurors. Moreover, too much data can also create legal and ethical issues, such as violating privacy rights, exceeding discovery obligations or compromising chain of custody.

Therefore, law enforcement and prosecution need a digital evidence management software (DEMS) that can provide a summary of the digital evidence in a concise, clear and consistent format, as well as to highlight the key evidence that supports the case. Such a software should be able to synthesize the data from multiple sources, such as ALPR systems, body cameras, drones, and community sources, into a coherent and comprehensive narrative, as well as to provide visual and audio aids, such as maps, charts, graphs and timelines to illustrate the evidence. Moreover, DEMS should be able to customize the summary according to the needs and preferences of the prosecutors, the judges and the jurors, as well as to comply with the legal and ethical standards of presenting digital evidence.

Using DEMS can make the prosecutorial process more effective and efficient, as well as more credible and persuasive, when it comes to digital evidence. This software can help to save time and work involved in preparing and presenting the digital evidence, as well as to improve the understanding and interpretation of the digital evidence. Moreover, DEMS can help to prevent or address any issues or objections that may come up from using digital evidence, as well as to guarantee the equity and integrity of the prosecutorial process.

Philip Lukens served as the Chief of Police in Alliance, Nebraska from December 2020 until his resignation in September 2023. He began his law enforcement career in Colorado in 1995. He is known for his innovative approach to policing. As a leading expert in AI, he has been instrumental in pioneering the use of artificial intelligence in tandem with community policing, significantly enhancing police operations and optimizing patrol methods.

His focus on data-driven strategies and community safety has led to significant reductions in crime rates and use of force. Under Lukens' leadership, his agency received the Victims Services Award in 2022 from the International Association of Chiefs of Police. He is a member of the IACP-PPSEAI Committee—Human Trafficking Committee, PERF, NIJ LEADS, Future Policing Institute Fellow and ASEBP Board Member. He holds a Bachelor of Science in Criminology from Colorado Technical University. He has also earned multiple certifications, including Northwestern School of Police Staff and Command, PERF's Senior Management Institute for Police, Supervisors Institute with FBI LEEDA, and IACP's Leadership in Police Organizations.