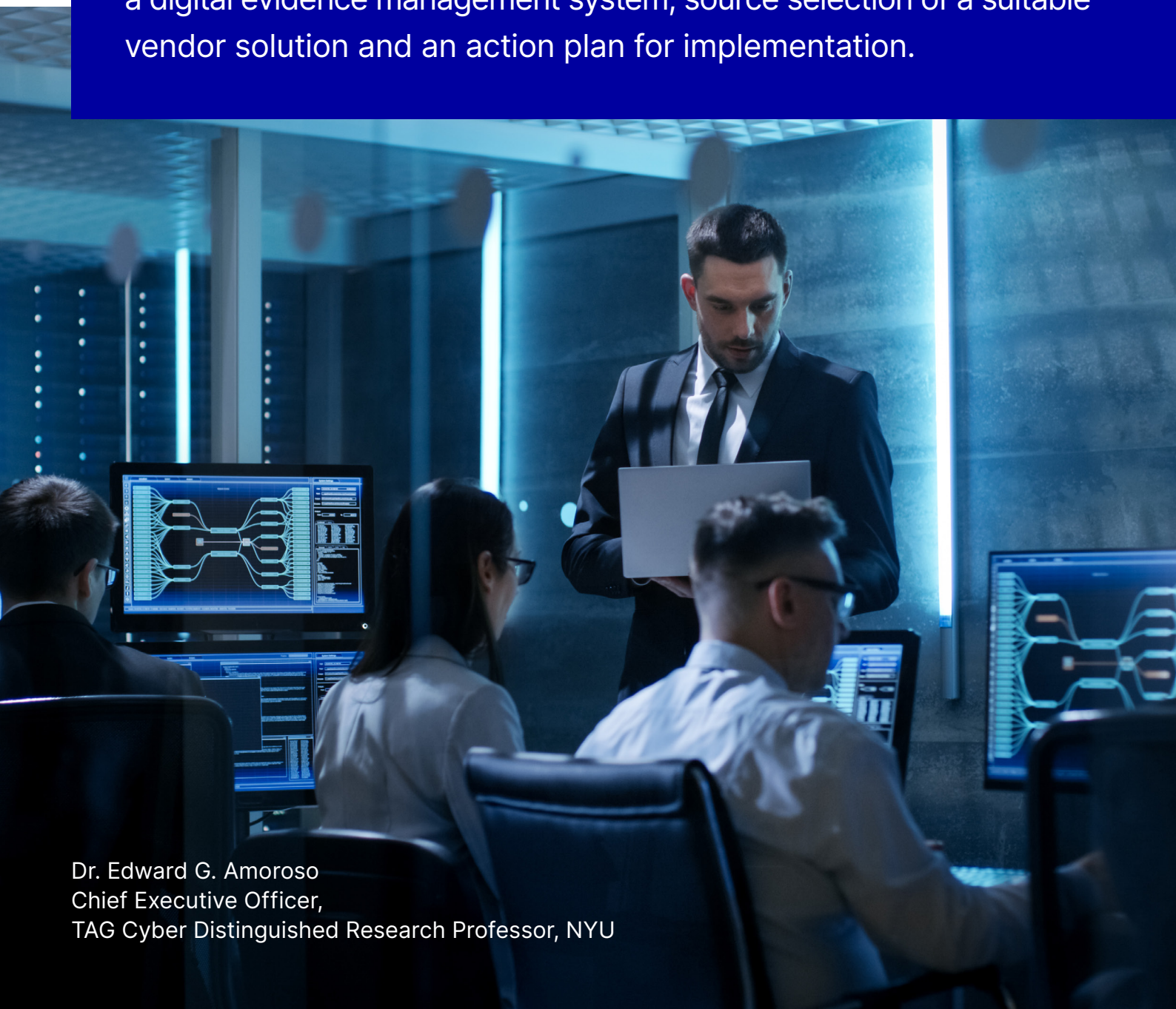
opentext™

TAG CYBER

WHITE PAPER

A model for digital evidence management

This digital evidence management (DEM) model supports the lifecycle requirements of law enforcement teams and other digital evidence stakeholders. It outlines platform requirements for a digital evidence management system, source selection of a suitable vendor solution and an action plan for implementation.



Dr. Edward G. Amoroso
Chief Executive Officer,
TAG Cyber Distinguished Research Professor, NYU

opentext™

Contents

opentext™

Introduction

Evidence management in law enforcement investigations is a complex topic studied, debated, and analyzed for decades across different local, state and federal contexts.[1] Traditionally, digital evidence was gathered from desktops, laptops and servers and consisted of various digital artifacts, some of which were created without the user's knowledge. With the recent proliferation of mobile devices, the availability, categories and sheer volume of evidence have increased. According to industry analysts more than 80 percent of the digital evidence recovered by law enforcement can come from mobile devices. Cloud computing is also changing the nature of digital evidence. It provides an inexpensive means for commercial application deployments, leveraging increased market availability coupled with scalable storage and processing power. As the adoption of commercial cloud applications continues to grow, so will the availability and importance of cloud-based digital evidence for law enforcement investigations.

Today, digital evidence commonly includes rich media, classic forensic digital evidence, digital documents and other electronic business records. As with all evidence, digital evidence must be properly collected, processed, stored and analyzed in a forensically sound manner to be admissible in court.[2]

Because modern investigations increasingly involve digital evidence, investigators must leverage software platforms to collect, manage and protect this evidentiary information and other artifacts. The question is how these tasks are supported and how the fidelity and integrity of the digital evidence is maintained in compliance with the Rules of Evidence. This is especially true when evidence has shifted from largely tangible components, such as weapons and stolen property, to massive amounts of digital evidence from different online, private and other sources.

In this report, we introduce a model for modern digital evidence management (DEM). The purpose is to assist law enforcement and other digital evidence users in selecting the best commercial platforms, or digital evidence centers, to support their work. We hope this DEM model will help law enforcement buyers and users differentiate between platform features and provide them with information to choose the best tool for their digital investigations.

1 For a brief introduction to this extensive debate see https://en.wikipedia.org/wiki/Evidence_management.

2. National Institute of Justice, *The Importance of Management in Evidence-Based Policing*, https://nij.ojp.gov/topics/articles/importance-management-evidence-based-policing

opentext™

Baseline digital evidence requirements

Policing and law enforcement have seen the requirements for modern digital evidence management evolve in the digital age. Digital evidence management enables law enforcement agencies to ingest, store, manage and analyze ever-increasing and varied digital evidence collected from body-worn cameras, mobile devices, laptops, servers, documentation physical evidence analysis and submissions from the public in a secure, efficient and legally admissible manner.

The best commercial providers of digital evidence management solutions support rich media, digital forensics, content management, law enforcement activity and modern extensions of these activities to mobile, cloud and SaaS-based services.[3]

To that end, experts suggest three categories of requirements that law enforcement buyers should focus on when reviewing DEM platforms.

Analysis support

Any platform considered for DEM should include support for digital evidence capture and analysis. Current digital evidence management systems typically focus on media generated from body-worn cameras, in-car videos and non-lethal defense weapon digital files, which have become instrumental for communicating law enforcement actions to the public. Available digital evidence currently collected by law enforcement during investigations is much broader than rich media and any digital management platform under consideration should incorporate support for analysis of these new digital evidence categories.

Digital evidence capture and analysis typically employs a familiar three-step process known as acquire-collect-analyze.4 In the first step, the targeted devices or systems are acquired and accessed using legal means. Historically, this meant physically seizing and isolating the device, but this approach has been extended to include access to virtualized systems.

Second, the data must be collected from the seized devices or systems. This process differs based on the circumstances of the investigation, targeted devices or systems and the type of digital evidence collected. Digital evidence collection typically involves the creation of a digital copy or accurate forensic image of the device or system data, with the original physical device or system evidence retained in an unaltered state to ensure proper chain of custody and admissibility. While

we generally refer to digital evidence in terms of video, audio, forensic or seized documents, it also includes reports, analysis results or images associated with processing physical evidence such as ballistics, blood splatter and DNA. This digital evidence is ingested and stored in a DEM system to facilitate access, analysis and collaboration by authorized users.

Once collected and processed, technical professionals with specialized skills and experience analyze physical and digital evidence using industry best practices and standards. They then share reports, diagrams, transcripts, lab results and other analytical products with investigators. A lack of skilled professional staff, higher volumes of evidence and the complexities of modern investigations make modern investigations more challenging.

3 The author consulted heavily in the development of this report with OpenText, which is the commercial provider of the iconic EnCase digital forensic platform, which has been the clear industry leader in digital forensics for many decades.

Technology is not sophisticated enough to replace the skills and capabilities of professional technical staff in processing and forensically analyzing digital evidence. However, technology can augment those capabilities and provide investigators with the tools to review, conduct additional analysis and collaborate on the resulting digital evidence to lessen the burden on already limited technical staff and systems.

For example, investigators may review body-worn camera footage in response to a complaint, screen video submitted by the public or enhance closed-circuit television images to identify a suspect or vehicle. Digital evidence technologies provide capabilities such as video and image enhancement, high-speed scrubbing and redaction, among others.

Although speech-to-text technology requires validation, it reduces the transcription burden and costs related to video interviews, interrogations and other audio files. Leveraging content management technologies, investigators can digitize documents, reports and business records and conduct targeted searches to identify persons, objects, locations and events using keywords, phrases, filters, metadata and tags or perform redactions as legally required. Technology augmentation provides investigators with a self-service model without requiring technical resources, which reduces workloads, improves investigative efficiency and speeds case closure.

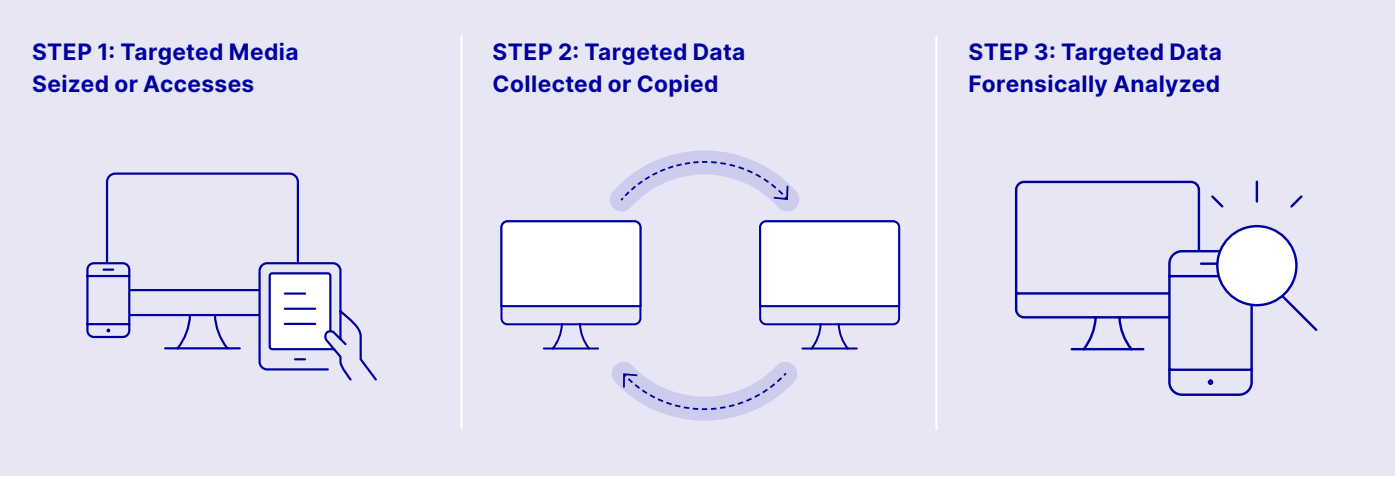


Figure 1. Digital evidence capture, copy and analysis

opentext™

Management support

Historically, assessing digital evidence management systems was focused on basic capabilities. As the proliferation of digital evidence, body-worn camera and other rich media increased, so did the need for a system to manage these different types of digital evidence. In response to growing demand, vendors often provided single-use products that increased the complexity, training requirements and operational costs required to manage digital evidence.

The management of evidence and the support processes were more like those used for physical evidence management. Classic management process considerations addressed legal accessibility, role-based access controls, inventory and storage controls, disposition and interaction with other law enforcement or prosecutorial agencies.

The current trend in digital evidence management systems incorporates a broader set of evidence management capabilities into a single platform integrating the management of multiple evidence types, multi-tenant user accessibility and technical professional augmentation. This enables self-service analysis, comprehensive audit capabilities for chain of custody and collaboration with the public and other law enforcement agencies in a secure manner.

As digital evidence management system capabilities have increased, so have agency management support requirements. When considering a DEM system, investigative agencies should consider new processes that address budget increases for system acquisition, storage and retention costs and integration with other law enforcement systems to gain efficiencies. Simplified training and interaction with suitable support groups, such as the National Criminal Justice Technology Research, Test, and Evaluation Center, should also be considered.

Security support

Law Enforcement agencies are increasingly adopting cloud-based digital evidence management solutions and other law enforcement support systems due to cost savings, improved processing performance, scalable storage, cyber security support, disaster recovery and business continuity services. The availability of analytic, reporting and other cloud-based technologies inherent in cloud providers is also a factor.

Collecting and storing digital evidence in an online repository means that cyber security protections must be carefully reviewed and strictly enforced. This is especially true for commercial platforms using public cloud infrastructure for digital evidence management. These cloud-based centers are convenient and ubiquitous, but also increase the importance of appropriate information security policies and compliance programs.

Security compliance is an essential consideration for cloud storage of digital evidence. Most law enforcement agencies will require compliance with the Criminal Justice Information Services (CJIS) Security Policy.[4] The CJIS policy is intended to guide the controls, policies, procedures, personnel and practices required to support law enforcement information services securely and safely. Fortunately, cloud providers who routinely support law enforcement provide CJIS compliant cloud environments with appropriate infrastructure and platform cyber security safeguards.

4 U.S. Department of Justice. *Criminal Justice Information Services (CJIS) Security Policy*, https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

Cyber security requirements that law enforcement and other users or stakeholders must consider in the selection and deployment of a digital evidence center fall into three main categories:

- **Digital encryption** – The data stored in a digital evidence repository is of obvious sensitivity and importance, so the use of encryption is essential. Data should be encrypted both in flight and at rest to help prevent unauthorized access or possible corruption of the evidence integrity. Hashing technology should be considered to support digital signature-based authenticity controls and tamper resistance.
- **Hosting security controls** – The hosting environment for any virtualized digital evidence repository must include the best available cyber security controls to ensure protected operations. This includes containerized segmentation, behavioral monitoring and strictly enforced access policies based on least privilege.
- **Strong authentication** – The most critical control in any hosted environment involves identifying and authenticating access. This includes user access to the digital evidence to support case management and administrative access to the repository for configuration, update, patching and other support tasks.

Figure 2. Security model for DEM infrastructure

opentext™

Introducing the DEM model

In general, digital evidence involves anything that provides helpful information to law enforcement teams independent of any physical devices, systems or equipment. This is not to say that such physical components are unimportant, but rather that a DEM system involves the storage of digital information.

The DEM model introduced here weaves the three categories of support requirements mentioned above into an operational model that matches the most common use-cases for law enforcement. They are ingestion, storage, evidence lifecycle management, analysis and collaboration with appropriate security support for all three types of digital evidence: media, forensic and documents.

Examples of digital media evidence include videos from body-worn cameras, in-car video, mobile device images, closed-circuit video files, audio files, interrogation or interview videos, 911 call recordings and non-lethal weapon data. General examples of forensic evidence include evidence or logical file images collected from desktop, mobile devices, cloud environments and sensors. These may include an operating system, application artifacts, mobile images, social media, emails, chat and text exchanges, network transmission collection and other virtualized data. Evidence obtained for other purposes through scientific methodology is also considered forensic evidence, but only the documented results are included in a digital evidence management system. Examples of documentary evidence include seized business records, forensic evidence reports, DNA, blood splatter, ballistics and fingerprint analysis, investigative reports, electronic transcripts and records management systems.

The security of digital evidence files must also be considered. This is often accomplished by isolating files during ingestion and using commercially available anti-virus tools, anti-ransomware software, threat scanning and other detection and remediation software. Encryption utilities protect the confidentiality of digital evidence files. At the same time, the integrity is ensured by calculating MD5 and SHA1 hashes of the extracted content and storing it as validation of the ingested digital file. A digital evidence audit trail contains the entirety of activity records that document each step in the handling, access, analysis, movement and cradle-to-grave lifecycle of each piece of evidence.

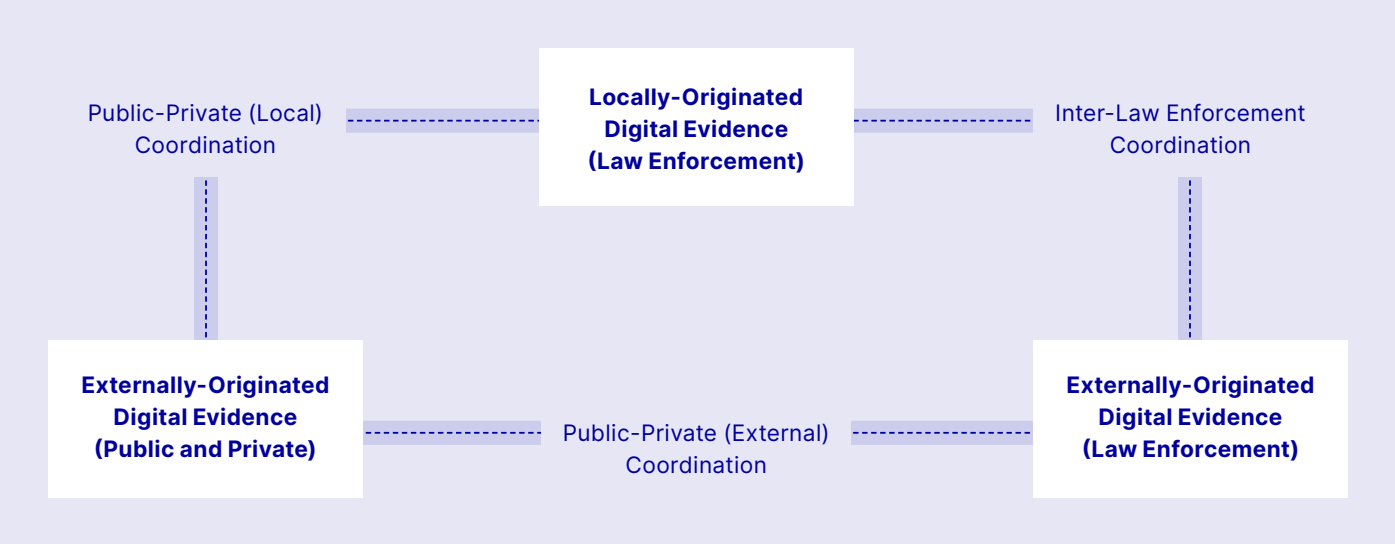


Figure 3. DEM Model for Law Enforcers

opentext™

Forms of evidence

Externally originated evidence

The primary digital evidence base comes from the familiar law enforcement process where information, artifacts, devices and other components are obtained legally and stored securely in the DEM system. Previously, this evidence base was collected from more physical mediums, including physical devices and printed documents. But recently, the base has shifted dramatically toward the greater inclusion of digital evidence.

Physical evidence is collected, processed and stored in consideration of best practices and agency policies. Physical evidence containing potential digital evidence is processed using generally accepted chain of custody rules and technical professionals to preserve and extract digital evidence. This digital evidence is then ingested and stored in a digital evidence management system while the original physical evidence is returned to the physical storage facility to ensure preservation of a proper chain of custody. This can include, for example, a cell phone found at a scene, digital evidence uploaded into the digital repository or physical evidence stored in evidence or a property room.

Local law enforcement evidence
Digital evidence collected, stored, processed and analyzed by the local law enforcement team with primary investigative responsibilities serves as the central component in the DEM model. Not only does it include the primary repository for all relevant evidence, but it also serves as the primary means by which all meta-data is coordinated, including chain of custody and related legal properties.

The interface between locally originated evidence and externally originated digital evidence from public and private sources, represents an important coordination of public and private domains. This can include open solicitation, partnership with organizations, messaging to the public and other commonly supported activities. The plethora of digital evidence created by citizens using smartphones and cameras highlights the importance of this interface.

Supporting law enforcement evidence

The digital evidence collected and processed by law enforcement professionals working outside the purview of the local law enforcement team will also represent a valuable resource in the DEM model. Modern computing and telecommunications bring geographically diverse law enforcement together via public and private networks, including the internet. As such, evidence collected by remote law enforcement rarely goes unnoticed by local investigative teams. This is supported by DEMs with multi-tenancy capabilities.

Buyers of commercial digital evidence support solutions should review any

multi-tenancy capabilities that support this collaboration. Desirable features include support for platform multi-tenancy, flexible access control mechanisms to enforce multi-dimensional policies, unique identifiers for collected data and evidence and highly configurable workflow support to integrate local and remote procedures.

The interface between local and external law enforcement has always been important, long before digital evidence even existed. With the proliferation of network sharing mechanisms and law enforcement databases, this interface has a new significance. The good news is that if some investigative body has collected evidence, the likelihood is high that it will find its way into the local repository central to the DEM model.

opentext™

It is worth noting that many commercial digital evidence systems are provided by vendors that sell body-worn cameras or in-car video systems. The best solutions will expand this traditional support to include forensic and documentary evidence. Also, scalability of storage, processing power and the ability to leverage analytics to automate processes, discover associated linkages and provide executive recording capabilities should also be considered in digital evidence management system assessment and evaluation process.

An action plan for implementation of the model DEM

The TAG Cyber team recommends that law enforcement teams and other stakeholders in the digital evidence lifecycle engage in a near-term action plan to optimize their support capabilities in this crucial area. This action plan can also be applied to implementation of the model DEM. The three steps to be included in this action plan are as follows:

STEP 1: Review existing digital evidence process

Law enforcement teams are advised to review the existing process for handling digital evidence with emphasis on whether such evidence is handled across the entire lifecycle. This includes collection, processing, analysis, review and all the various tasks outlined in this report. Each of these steps should be documented, and their respective interactions and dependencies should be clearly defined.

STEP 2: Develop platform requirements for digital evidence

Law enforcement teams are advised to develop a set of local requirements for digital evidence platform support based on the DEM model. These platform requirements should include support for workflow automation, but they might also address modern content management capabilities. The requirements should be reviewed in the context of existing vendor support, as well as potential new commercial offerings.

STEP 3: Talk with vendors about an integrated solution

Once the existing digital evidence lifecycle is documented and platform requirements have been created based on the DEM model, the law enforcement team will be ready to begin talking with vendors about their present and future capabilities. The key issue for a DEM-based digital evidence center is a high degree of integration between digital and conventional evidence systems.

This integration should include an application programming interface (API) strategy allowing integration with other law enforcement systems to extract complaints, incidents or investigative case-relevant evidence. Law enforcement buyers should also ensure that selected platform solutions support the provision of notification of disposition from court to agency to property and evidence rooms.

STEP 4: Consideration of budget constraints

The use of disparate systems for document management, rich media management and forensic evidence management has a significant impact on law enforcement budgets in terms of not only product and solution costs but staff training and support costs as well. As law enforcement budgets are under increasing pressure, agencies should consider the efficiency and cost advantages of a digital evidence management solution, along with the capital, personnel, training and maintenance impacts to budgets.

opentext™

Learn more

About TAG Cyber

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn

opentext.com/contact