Analysis of the Law Enforcement Digital Evidence Imagery Lifecycle

The IJIS Institute Law Enforcement Imaging Technology Task Force

Table of Contents

Acknowledgments

This document is the product of a partnership between the IJIS Institute and the International Association of Chiefs of Police (IACP). We would like to thank the members of the Law Enforcement Imaging Technology Task Force (LEITTF) for supporting the creation of this document:

IJIS Institute Law Enforcement Imaging Technology Task Force Members

Patrick Doyle, *LEITTF Chair and Vice-Chair, IACP CJIS Committee*
Paul Spencer, *LEITTF Vice-Chair and Chief of Police (retired), Addison, Texas Police Department*
Craig Allen, *Chair, IACP Communications and Technology*
Ben Bawden, *Brooks Bawden Moore*
Jim Buckley, *Chair of the IJIS Law Enforcement Advisory Committee*
Amy Bundens, *Tyler Technologies*
Michael Burridge, *Police Chief, retired.*
Terry Clark, *International Association of Chiefs of Police (IACP)*
Susan Crandall, *Motorola Solutions*
John Dowden, *NEC*
Susan Goleman, *Tyler Technologies*
Robert E. Greeves, *National Criminal Justice Association*
Glenn Hanson, *Chief, Marble Falls Police*
Jenner Holden, *Axon*
David Jackson, *Issured*
Karisa Longo, *Intern*
Catherine Miller, *Program Manager, NCR-LinX, Montgomery County Police Department*
Mike McDonald, *Motorola Solutions*
Rex Pagerie, *Fairfax County Police Department, Virginia*
Chris Pogue, *Nuix*
Dave Russell, *Fairfax County Police Department, Virginia*
Mike Sena, *Northern California High Intensity Drug Trafficking Area and Northern California Regional Intelligence Center (NCRIC Fusion Center/HIDTA)*
Tanya Stauffer, *Innova Solutions*
Jed Stone, *Issured*
Robert Turner, *CommSys*
Jerry Ward, *Mission Critical Partners*
Heather Whitton, *Cincinnati Ohio Police Department*
Karl Wilmes, *Federal Heights Police*

The following IACP members also contributed to the content of this paper:

Jim Emerson, *Chair, IACP Computer Crimes Committee, NW3C*
Glenn Hanson, *Chief, Marble Falls Police*
Keith Kelley, *IACP, Deputy Chief, Athens-Clarke County Police*

Comments and Questions? They are always welcome! Please contact the IJIS Institute at **info@ijis.org** or **703-726-3697**.

Executive Summary

The IJIS Institute's Law Enforcement Imaging Task Force (LEITTF) was asked to determine how the criminal justice system could best address challenges specific to Digital and Multimedia Evidence (DME) within the siloed redundant lifecycle of law enforcement, prosecution, and the courts.

This paper answers key challenges including; how to apply Chain of Custody standards across the criminal justice system; what would be the impact on law enforcement and the criminal justice system if digital evidentiary material was accidentally or purposefully lost or disseminated; who has custody of the digital evidence at various stages of its lifecycle and what are their responsibilities to the digital evidence within the lifecycle; and what are the various perspectives and use cases for stakeholders across the criminal justice enterprise as it relates to digital evidence?

Within this paper, the LEITTF focused on considerations for DME captured by law enforcement agencies for use in criminal cases although it follows from the above that the scope could encompass both criminal and civil cases and all the applicable relevant parties.

While the need to manage DME is growing and changing, the underlying processes of evidence management remain the same: Collect, Vet, and Disseminate. The LEITTF has attempted to describe the considerations that agencies should evaluate as they work with their criminal justice partners to support their mission. The considerations presented herein should spur discussions with agency partners regarding these immediate and long-term challenges.

This document is intended to provide general guidance, assistance, and help to professionals in the broader criminal justice community. That said, there will be investigative, administrative, or legal considerations requiring exceptions.

Background

The Law Enforcement Imaging Technology Task Force (LEITTF) is a joint effort of the IJIS Institute (IJIS), and the International Association of Chiefs of Police (IACP) Criminal Justice Information Systems (CJIS) Committee Computer Crimes and Digital Evidence Committee.

Previous joint efforts between IJIS and IACP have produced research on license plate reader systems success stories, management practices, user surveys, and RMS Functional Standards. The LEITTF has also produced examinations of facial recognition use cases and model policies while also making contributions to many other white paper documents on various law enforcement technology topics.

Introduction

During research endeavors over the past several years, the LEITTF discovered emerging challenges to all aspects of Digital and Multimedia Evidence (DME) collection, vetting, and dissemination, as well as the overarching processes of management and Chain of Custody. The LEITTF also found limited awareness of best practices and few seamless transfers of DME between stakeholders in the criminal justice system. The LEITTF began this effort to analyze the Lifecycle of Law Enforcement DME as a result of these emerging challenges. The content of the document is intended to offer considerations for leaders in the criminal justice community as they integrate DME into their business practices.

The Lifecycle of DME is complex and affects many stakeholders, some of whom have competing objectives, all of whom have differing requirements, use cases, and time horizons. The LEITTF's goal in this white paper is not to be prescriptive rather the goal is to provide readers insight into the complexity of the various use cases and issues that should be considered to support the effective use and management of DME throughout the criminal justice system.

Problem Statement

Digital media technologies and adoption are proceeding at a breakneck pace, creating both challenges and opportunities for law enforcement, prosecutors, and the courts. It is clear that evolving digital media technologies are increasing demands on the criminal justice system for four key reasons:

1. The explosion of affordable video technology is rapidly growing the number and types of sources of DME, both for public safety agencies and the citizens they serve. In addition to the affordability of video capture is the fact that video and digital photo editing have become more prevalent.
2. Public demand for instant definitive evidence (the "CSI" television show effect) is increasing prompted by infamous cases in the news headlines featuring videos of police or criminal activity.
3. The broader society has digitalized, and the criminal justice processes are now playing catch up. This is impacted by the rapidly advancing use of digital devices such as body-worn cameras (BWC) under a wide array of governance and usage policies.
4. The everyday digital fabric in which our lives are woven makes it seem that assets are easy to handle, share, and socialize when, in fact, for governments, this is often not the case.

Equally clear is that the criminal justice system is not well equipped to cope with these changes. There are several complex root causes. The LEITTF believes the underlying issues can be grouped into three broad classes. Chief among these issues is one central fact: digital evidence is different from physical evidence, for which well-understood rules apply. Unlike physical evidence, digital data can be copied, altered, or corrupted if not properly managed. There exists a parallel set of standards and security measures that apply to DME that align with the realm of physical evidence. Secondly, the gaps in software applications that support the criminal justice process are exacerbated further when digital evidence is involved. It is important to note that whether evidence is physical or digital, there is a standard continuum of management: identification, collection, preservation/custody, analysis/evidentiary production, and reporting. The challenge with digital evidence is the disparity or incomplete presence of these functions among various tools and technologies used by and throughout the criminal justice process.

Finally, across the entire criminal justice system, there is a challenge in implementing policy to address digital evidence management in advance of technology deployments.

Reflecting on these issues, it became evident that all stakeholders would benefit from a better understanding of the use cases and differing requirements for DME at each stage of the criminal justice process by including insight into the challenges and constraints (financial, technical, operational, and even societal) faced by users at each stage. By examining the issues raised throughout the digital evidence lifecycle, the LEITTF hopes to enhance understanding of the issues and thereby enable stakeholders to meet the challenges by making shared decisions that improve efficiency and reduce complexity.

It should be apparent that it would be impossible in a short paper to offer prescriptive recommendations on specific issues. The LEITTF believes users will gain more from understanding the issues and being better informed to develop local solutions.

Finally, the LEITTF thanks the many participants who have contributed to these discussions and invites you, the reader, to engage further with the LEITTF either through feedback to the authors or by engaging with IJIS and the IACP.

Research Intention

The LEITTF was driven to ask how the criminal justice system could best address challenges specific to DME within the lifecycle and focused on the core questions such as:

- How do we apply Chain of Custody standards across the criminal justice system?
- What would be the impact on law enforcement and the criminal justice system if digital evidentiary material was accidentally or purposefully lost or disseminated?
- Who has custody of the digital evidence at various stages of its lifecycle and what are their responsibilities to the digital evidence within the lifecycle?
- What are the various perspectives and use cases for stakeholders across the criminal justice enterprise as it relates to digital evidence?

Definitions and Parameters

The scope of a paper discussing digital evidence runs the risk of attempting to address an impossibly broad array of issues. For example, the National Institute of Justice ("NIJ") defines digital evidence as follows:

> *"Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, a personal digital assistant (PDA), a CD, and a flash card in a digital camera, among other places. Digital evidence is commonly associated with electronic crime, or e-crime, such as child pornography or credit card fraud. However, digital evidence is now used to prosecute all types of crimes, not just e-crime. For example, suspects' e-mail or mobile phone files might contain critical evidence regarding their intent, their whereabouts at the time of a crime, and their relationship with other suspects."*[1]

To the list above we could add, without exhausting the possibilities, ATM transaction logs, instant message histories, spreadsheets, Global Positioning System tracks, logs from a hotel's electronic door locks, etc.

1 – https://www.nij.gov/topics/forensics/evidence/digital/pages/welcome.aspx

The UK National Police Chief Council's Digital Intelligence and Investigation Programme established that every crime, including most analog crimes, will now contain digital evidence.

Therefore, for this paper, the LEITTF has chosen the following definition of DME:

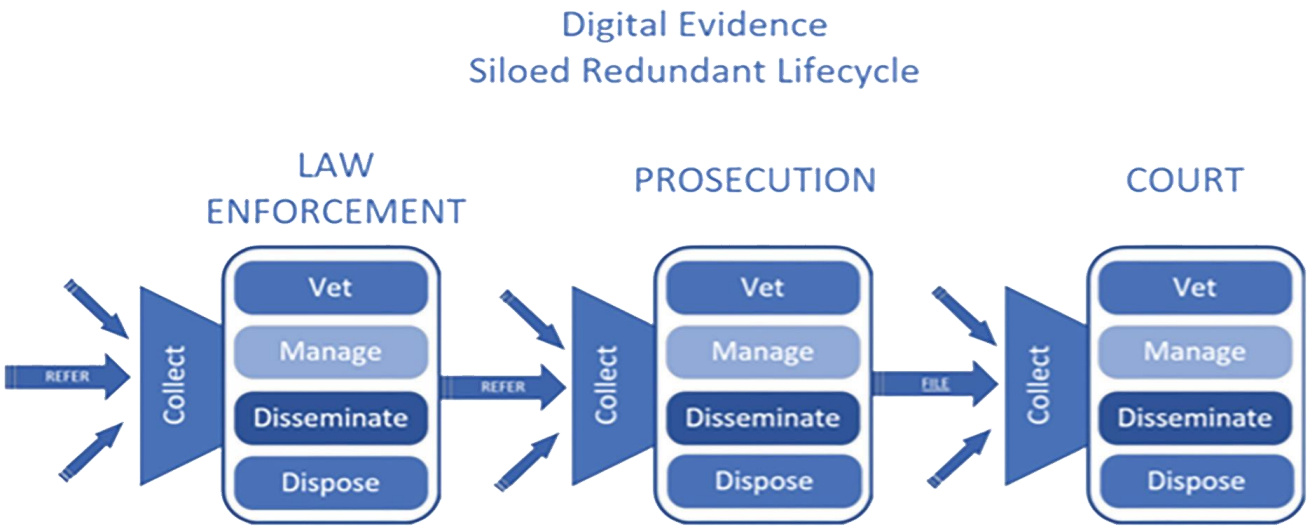
> *"Digital and multimedia evidence includes information on computers, audio files, video recordings, and digital images. This evidence is essential in computer and Internet crimes but is also valuable for facial recognition, crime scene photos, and surveillance tapes. NIST researchers are developing tools, measurement methods, standards, and data to support forensic analysis of digital evidence."*[2]

Within this paper, the LEITTF focuses on considerations for DME captured by law enforcement agencies for use in criminal cases although it follows from the above that the scope could encompass both criminal and civil cases and all the applicable relevant parties.

This document is intended to provide general guidance, assistance, and help to professionals in the broader criminal justice community. That said, there will be investigative, administrative, or legal considerations in any case, requiring exceptions.

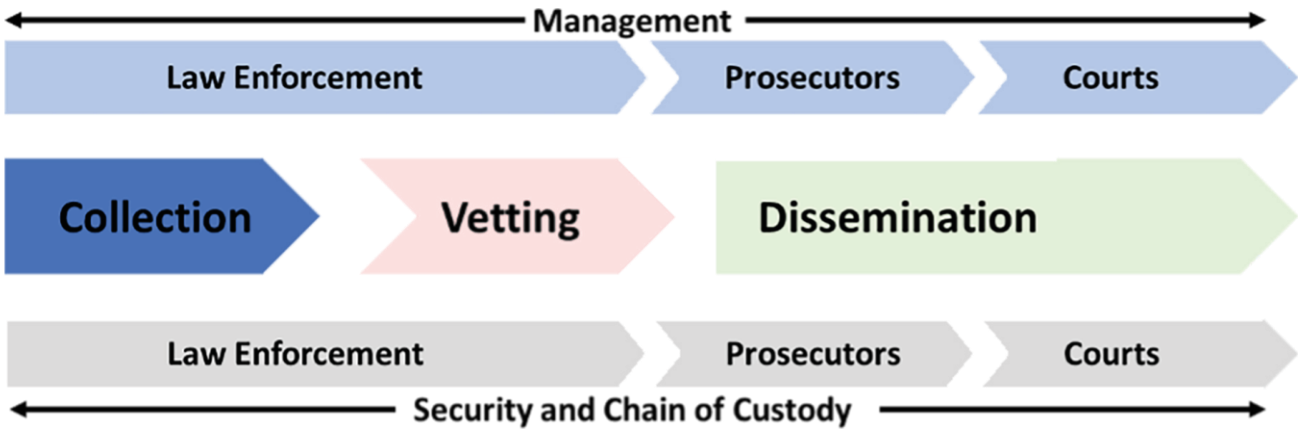
Key Concepts

The LEITTF determined the current general state of the DME lifecycle is siloed and fragmented, with many functions repeated by each stakeholder. There is little to no business efficiency passed along to other stakeholders regarding vetting, management, or analysis functions. There are exceptions, with some jurisdictions collaborating more than others, but there are examples of criminal justice communities that have fully developed policy and governance supported by the associated applications. The image below depicts the most common form of digital evidence lifecycle in jurisdictions we reviewed:



2 – NIST definition of Digital Multimedia Evidence - www.nist.gov/forensic-science/digital-and-multimedia-evidence#:~:text=Digital%20evidence%20includes%20information%20on,video%20recordings%2C%20and%20digital%20images

The diagram above illustrates that different stakeholders are often performing the same tasks, repeating work already done by others. Following extended discussion, the LEITTF determined that a better framework, as shown in the diagram below would help discuss more effectively common issues and look for synergies between stakeholders.



Accordingly, the paper is organized around the framework above, discussing policy and technical considerations at each stage.

- Process Stages
  - Collection
  - Vetting
  - Dissemination
- Overarching Processes
  - Management
  - Security and Chain of Custody

Process Stages

Collection

Introduction
The collection of DME is primarily an issue for law enforcement agencies; however, prosecuting attorneys and defense counsels do occasionally obtain evidence. Nevertheless, prosecutors and courts will be interested in the issues faced by collection agencies if only to ensure these are being addressed effectively and thus reducing risks around the challenges of evidence at later points in the justice process.

As discussed above, our primary focus is on the collection of DME (see Problem Statement Section), extended to cover additional types of evidence where the issues are similar. This section looks in detail at the minimum requirements of storage collection repositories and recommended workflows to ensure digital evidence, like physical evidence, is accepted in a trial court or other judicial proceeding. The LEITTF continues with a discussion of general agency policy concerns for the collection of digital evidence and ends with data conversion, system compatibility issues, storage limitations and options, and acceptance of various video formats. The growth of digital evidence introduces new challenges (compared to the processes in a traditional evidence room) and opportunities. In each case, we endeavor to highlight the issues that need to be considered and, where possible, offer examples of successful innovations that are helping agencies to evolve their processes. Our review of Collection issues looks at the following topics:

- Scope of Collection – Sources of Digital Evidence
- Sources - Law Enforcement, Citizen Contributors, Businesses and Municipalities
- Policy Considerations
- Data Conversion (existing to new), System Compatibility, Storage Limitations, and Storage Options
- Accepting Various Formats of Video

Scope of Collection - Sources of Digital Evidence

In its most simplistic form, digital evidence is any information that exists in an electronic format and has value to an investigation. Digital evidence includes information transmitted or received from computer systems. These systems may include computer servers, desktop and laptop computers, tablets, and smartphone devices. Digital evidence may be in the form of data files, text, audio, video, and image files, as well as data created by vehicles, telematics, unmanned aerial systems, and sensor data.

Digital evidence can also be generated from systems maintained by public safety organizations, such as computer-aided dispatch (CAD) systems, call processing solutions, digital recording solutions, body-worn cameras, vehicle cameras, public safety camera systems, and automated license plate readers (ALPR).

Sources - Law Enforcement, Citizen Contributors, Businesses and Municipalities

In this Digital Age, a variety of devices, types of content, and sources of collection and submission to a law enforcement agency are all potential components of an agency's digital evidence workflow and evidentiary repository. Agencies may elect to begin by collecting and storing content only from devices owned by the department and issued to their officers. Other agencies may be in a position to expand the sources of their collection by seeking partnerships for digital evidence contributions from the general public and businesses that installed security cameras at locations throughout their jurisdiction. The degree to which an agency begins its journey is driven largely by comfort, funding, infrastructure, and internal staffing to provide support for its chosen implementation level. Physical evidence collection will continue to be a significant part of a law enforcement agency's operation, but the evolution of this process to now include digital content has taken the traditional evidence storage room defined by four walls to an indiscernible and inconspicuous repository defined by gigabytes, terabytes, petabytes, and beyond.

The digital evidence collection process still requires proper documentation and a Chain of Custody that must be preserved up to and including the submission of that evidence in a court of law. While tangible physical evidence was generally photographed first before being removed to a property room, other documentation to support the evidence and its relevance to a case included the date and time it was reported, the date and time it was collected, the location of where the evidence was found and any specificity within the location, who found it, who collected it, a description of the evidence, the quantity of each item collected, the condition of the evidence when found, the case name, and the case number. The documentation involved in the contemporary collection of digital evidence largely automates the collection of many of these individual metadata items, thereby eliminating the cumbersome manual documentation or data entry process of the past.

Sources of law enforcement evidence collection have most recently been defined primarily by body-worn cameras, in-car video systems, mobile phone devices, and digital cameras. One of the early uses of digital cameras was to document injuries to victims of abuse in domestic violence cases. Cell phones or smartphones evolved to offer increased photo resolution quality defined by the number of megapixels. Primarily, except for special evidence collection unit personnel, the use of the digital camera has been replaced by personal or agency-issued smartphones having higher resolution cameras, allowing an officer to take photos or videos of encountered evidence very easily in their cases. Body-worn camera acquisition and use have exploded in demand by agencies seeking to neutralize one-sided viewpoints of police interactions with the public and to ensure officer accountability. These devices help to provide the full context of such interactions that can support meaningful conversations while also enabling transparency and accountability to the communities served by the police. In-car video systems, the precursor to the individual body-worn camera, provide the same context and transparency while offering a documented timeline of events in prosecutions with an "unbiased eyewitness" to support an officer's sworn testimony of incidents resulting in arrest or allegations of police misconduct.

Digital evidence can come from a variety of sources in a law enforcement agency, all related to criminal justice or the administration of criminal justice. These can include citizen engagement applications, 9-1-1 call transcripts (voice to text), radio communications logging, CAD events, access controls, video management systems, ALPR, Body Worn Video, In-Car Video, video security, and workflows of electronic systems involved in the documentation and investigative steps leading up to an arrest. All of these can make their way into a case file supporting an immediate prosecution or even a long-term investigation that could yield solvability factors long after the crime has been committed. Regardless, digital evidence identification, collection, storage, management, Chain of Custody, presentation, and validation are all necessary and critical features of a digital evidence management system that is the electronic equivalent of the physical property/evidence storage room in each department.

Private and other third-party contributors of digital evidence to the police, such as private businesses and homeowners, should ensure there is a clear understanding that their assistance is voluntary, and agreements should be crafted laying out the specific arrangement they have with the police to view, acquire, and use any evidence provided. For example, some agreements only allow the police to access a registered camera when an incident has occurred where the homeowner's camera may have captured the incident and possibly those involved. Other agreements allow for access at any time, and others only upon written permission of the homeowner. To the extent the parties will agree, indemnification clauses should be part of such agreements to protect either party should the other act inappropriately or contrary to the written agreement thereby exposing either party to litigation.

No matter the source of the digital evidence, the process should be well documented in policy that is routinely reviewed and improved upon to ensure privacy protections are in place and followed. Like the physical property room for non-digital evidence, the digital evidence repository, or digital property room, is just as important, if not more, as the devices capturing the evidence. The back-end solution that manages an agency's digital evidence needs to provide security, privacy, evidence continuity, Chain of Custody logging, case management, redaction, secure storage, secure sharing, and policies for retention, purging, and expungement.

A law enforcement agency must have policies in place to deal with not only their digital evidence collection systems and processes but also the collection, transfer, and storage of digital evidence captured on devices outside of their control. Ensuring the security and integrity of digital evidence collection requires having a set of well-defined policies supported by documented business processes with detailed procedures. As the pace of technology evolution continues to accelerate, these policies, processes, and procedures must be reinforced through ongoing and proactive reviews, coupled with a robust strategy for continued education of agency personnel.

Policy Considerations

As it relates to evidence, the primary role of law enforcement is to gather evidence and ensure that it is securely transmitted to a known repository while maintaining a record of the Chain of Custody. With physical evidence, the acts of collecting, transporting, and managing a record of the Chain of Custody are relatively easy to articulate and understand. Digital evidence, however, can be collected from multiple types of digital devices (closed-circuit video systems (CCTV), body/dash cameras, DSLR cameras, mobile phones, and thumb drives). Only some of these devices are under law enforcement control, requiring different approaches to addressing the concepts of collection and Chain of Custody.

The primary areas that an agency should evaluate and provide policy for digital evidence collection systems are:

- Which applications and devices are considered "safe" for collection?
- Which applications and networks are considered "secure" for transfer?
- How are conversion, redaction, and annotation performed?
- Where should the digital evidence ultimately be stored?

Additionally, all these factors should be evaluated through the lens of Federal and State/Provincial requirements for secure data.

"Safe" Digital Evidence Collection

Digital evidence collected by citizens has exponentially increased in the last decade. Mobile phones with embedded cameras are now ubiquitous. Home surveillance systems and video doorbells have become affordable and much more commonplace. There is no possibility to require only certain "certified" applications for these devices to collect their digital content. The issue will be how an officer can quickly and easily collect those digital assets from the citizen, yet still maintain authenticity and a Chain of Custody. That topic is addressed in the agency policy section below related to "secure workflows" for the transfer of digital evidence.

Law enforcement agency-issued devices for digital evidence collection typically fall into two categories: dash/body cameras and digital cameras. Those devices have matured dramatically in the last decade. Any vendor with a modern platform is likely to provide more than adequate methods of collection on their devices that will result in high-quality digital content.

While most law enforcement agencies do not issue their officers smartphones, many law enforcement officers will carry a personal smartphone device. The question then becomes, if an officer is at the scene of an incident and doesn't have easy access to an agency-issued device with a digital camera, should the officer be permitted to use their personal device to capture digital evidence from the incident? This question should be addressed in that law enforcement agency's jurisdiction as a matter of policy. Ultimately, it would be the prosecutor who may have to prove in court how that piece of digital evidence was captured. Having their buy-in on the topic of using an officer's personal smartphone articulated in policy for the law enforcement agency would be of benefit to both offices.

Today, there are modern capture applications available for smartphones with respect to law enforcement uses in evidence collection that never stores the captured media on the device. The app is merely the mechanism to capture and securely transmit the evidence to the approved repository. The picture or video is not stored on the device and cannot be seen in the photo library on the device either. It cannot be deleted from the smartphone app; it can only be uploaded to the repository. In short, these modern apps are only the capture and transport mechanism for the photographed evidence, and this capability virtually eliminates the possibility of the officer's personal phone becoming discoverable or seized as part of a defense motion. Like established legal theory, though, nothing is absolute, and therefore, it is strongly recommended that this exception be thoroughly discussed with an agency's prosecution team for their legal opinion regarding their concurrence or rejection.

"Secure" Workflows for Digital Evidence Collection

Another area of policy that should be addressed is how digital evidence gets transferred from the collection point/device to the repository.

This is mostly a solved problem with modern body/dash camera solutions. These devices can automatically upload to the law enforcement agency's repository using a secure method of transport. As for digital cameras, the evidence is typically transferred directly from the memory card or device memory to the repository via an agency laptop/desktop. However, the most current digital body-worn and in-car camera devices can upload content directly to the repository with an installed cellular SIM card or connection to a broadband modem in the vehicle.

Capturing citizen data securely requires a different approach. Email and text are generally not adequate due to security concerns, size limitations, and email filtering software. Citizens can bring their devices to the agency, but this can be cumbersome and time-consuming. Other methods need to be considered such as capturing citizen data through a secure web portal that requires authentication and has a workflow for automated virus scanning and vetting for relevancy.

Having the ability for citizens to go to a website after leaving the scene of the incident and upload information is useful but potentially fraught with additional steps. The citizen may forget, and the officer is then burdened with trying to track down the person later. While the citizen may still need to be prompted, having a mechanism to "invite" the citizen to upload their files by using a secure link (e.g., a business card with a QR code, the ability to send a text message or email invitation) is a better way to ensure that as much citizen-captured digital evidence is collected as possible.

To any vendors looking to build applications for law enforcement officers to safely collect and securely transfer digital evidence from devices not under law enforcement control, such as cell phones, the primary tenet is ease of use. For the safety of the officer and the public, the officer can't be focused on the tooling. They must be focused on the situation and the people. Any application built for collecting digital evidence in the field should trend towards fewer, simpler, and more obvious-to-use features. Advanced or complicated actions that might require more focus and extra clicks or swipes could still be in the application but should not be in the officer's workflow for the most common actions.

Storage Options for Digital Evidence Collected

Security, as well as the cost of ownership, of any digital evidence repository, are important factors for a law enforcement agency to evaluate before deciding on a solution.

Data, including digital evidence, is now more commonly stored "in the cloud" as opposed to a set of on-premise servers. Concerns about the lack of security for this method of storage are becoming outdated. Multiple cloud storage vendors have solid security track records and high-level security certifications that can often surpass what a local IT shop can support. Agencies should determine which certifications are important and ensure that the cloud vendor can provide the agency with proof of these certifications.

Digital evidence storage and backup needs can eclipse typical data storage needs for an application like a records management system (RMS). When evaluating the total cost of ownership of using an application that supports cloud storage versus buying and maintaining an on-site server farm, cloud storage is likely the more flexible and affordable option over time.[3]

3 – Connectivity costs could be higher especially if redundant connections are important.

Some additional benefits of cloud storage that apply to cost may include:

- Disaster recovery plans are based on large, reliable, and scalable infrastructures that are included in the cost of the maintenance plan.
- The ability to "price as you go", which means your agency doesn't have to purchase all the servers it needs upfront and can ramp up costs over time instead of a large initial outlay.
- Very quick responses to providing additional storage requirements, as opposed to having to procure and provision local storage devices.
- Some cloud vendors support the automatic transfer of less frequently retrieved files to less expensive storage, which can help keep the overall costs down over time.

One of the drawbacks of these very flexible cloud storage options is that it's often difficult to confirm an actual cost from a cloud storage vendor. More specific pricing can be determined if an agency can quantify how much digital evidence is expected, how fast it will grow in size, and how often it will be accessed. If an agency is primarily using thumb drives, CDs, DVDs, and Blu-rays today, specific storage needs may be difficult to determine and may take some best guesses. The law enforcement agency should review the growth of its storage needs and costs regularly.

Despite strong security measures that are in place for the major cloud storage vendors, some agencies still do not feel comfortable having data, like digital evidence, in third-party systems. In this situation, the only option is to have servers on-site for storage and backup, as well as the staff to fully secure and support them.

Data Conversion (existing to new), System Compatibility, Storage Limitations, and Storage Options

In many cases where law enforcement has been storing digital evidence, there has been an evolution in practice and policy over time to duplicate the physical property room procedures that have generally served criminal justice well. When agencies first began capturing digital evidence in the late 80s and early 90s, officers would securely collect the evidence, but their department rarely was able to provide a repository for its storage. In short, officers collected available evidence on whatever medium they were familiar with or what limited capabilities their agency provided, including CDs, DVDs, and thumb drives. Without a digital evidence management solution, it was either uploaded to a hard drive on a network device or kept in a drawer or file cabinet with the investigative report on the medium it was captured or submitted. Such practices gave way to formal security control-compliant solutions as the authenticity of the evidence, its continuity, Chain of Custody, and original integrity were questioned or challenged in the courtroom. Departments accumulated significant amounts of videos, pictures, documents, and sometimes in a variety of formats. When they finally purchased back-end solutions, the agency needed to decide what evidence was still relevant and important to active cases that had yet to be decided or were pending appeal. As data storage systems began to mature and the cost of data storage began to decline, agencies invested in solutions that were generally on-premises and used as the central repository for all digital evidence. Cloud solutions were emerging, and up until about 2015, agencies resisted cloud solutions, fearing that they were less secure and presented a risk they were not prepared to accept. Fast forward to today, where cloud solutions, including cloud digital evidence solutions, are commonplace and widely accepted and are more secure, cheaper, and no longer the cost driver to agency budgets that on-premises solutions have become.

Agencies that accumulated video from one vendor's solution sometimes make a change to another solution and wish to move their old files to the new system. This could entail significant costs and inconvenience to the agency; especially if the stored format is different than the new system or is incompatible with the new solution. While the repository will likely store the alternate format without any problem, users may have to convert such video to what is likely an .mp4 format or other types such as .AVI or .MOV with an available open-source video player. Regardless, agencies often want to maintain their video repositories when changing vendor solutions, and this, in most cases, should not be problematic. System compatibility from old to new should be investigated and can usually be accomplished. When using vendor-supplied solutions and an agency decides to make a change from one vendor to another, this should generally not be a problem, provided each vendor works with the other to ensure a secure and complete transfer from the previous solution. Generally, this transfer can be done without too much effort and can be accomplished via electronic transfer from one system to the next with a provided API (Application Program Interface) or by exercising a contractual clause that should be a part of all vendor/customer agreements whereby the customer's data is returned to them in a pre-specified format or in the same format it was submitted to the current vendor.

Most commercial digital evidence solutions available to law enforcement today, whether it is an on-premise solution or a fully hosted cloud solution, should be capable of storing any digital content, including documents, audio files, pictures, and video. Forensic images of digital content on, for example, a hard drive, cell phone, or other device are usually challenging to maintain the file structure of the device's content. Today, providers of digital evidence repositories are at a distinct competitive advantage when they can maintain the file structure of digital content of such devices when importing these files into the repository. Agencies who require this functionality of their product providers will be able to better defend the veracity of the original capture of DME.

There really should be no technical storage limitations an agency should encounter today, particularly when a cloud solution is chosen. Most of the limitations encountered today will likely be financially driven or a function of space and time to adjust, as might be the case in an on-premises solution where the data center owner's space is maximized, and considerable time may be required to consolidate existing systems on shared servers (virtual environments) before additional capacity is available. With proper management and monitoring, these latter situations should be rare and most likely already projected and forecasted for change well ahead of any need.

An important consideration when trying to play digital video over the internet is whether the server/system hosting the data has streaming capabilities. Streaming allows instant playback of a very large video file, and the ability to quickly skip to a particular frame. Without streaming commercial video services such as Netflix or YouTube would not be possible. All modern DEM systems can stream video data that is stored in certain common formats. Streaming dramatically affects performance and bandwidth requirements, and without it working with large video files, it is cumbersome at best.

Storage options include on-premise storage, hybrid (combination of on-premise and cloud), public sector cloud (government cloud), and private cloud environments. Law enforcement agencies will either use on-premise storage solutions or if not cloud-averse, will choose government cloud solutions. Government cloud solutions are either CJIS Security compliant, FedRAMP certified, or both, and stem from the controls dictated by the security policy requirements they fall under, particularly in shared management data environments related to information sharing between local, state, tribal, and federal criminal justice agencies. Whether cloud or on-premises, these security policy requirements are critical. Agencies are encouraged to confer with their state Chief Security Officer regarding the information quality and technical security controls that apply to their agency. At a minimum, agencies should pursue NIST 800-53 Pub conformance. In addition, FIPS 140-3 will likely be required for encryption.[4])

4 – These are controls that focus primarily on federal requirements. Agencies need to evaluate and incorporate other controls that are applicable to their local and state jurisdiction.

Accepting Various Formats of Video

In today's law enforcement environment, when the term "Collection of Digital Evidence" is heard, most people think of computer-related or produced evidence. While important to many investigations, this thought leaves out the most widely gathered digital evidence today: video. Video is gathered from crime scenes, cellular telephones, social media sites, and home and commercial surveillance systems. It is estimated that more than 80% of criminal investigations today involve video of some sort.

While the opportunity to receive video evidence from crime scenes is beneficial and often leads to arrests and convictions, there is an inherent danger that most law enforcement officers are unaware of. Many manufacturers of video recording equipment, whether in a cellular phone or surveillance system at a convenience store, have a proprietary way of recording digital video. CCTV systems often have multiple cameras and often create a proprietary multi-stream file. Additionally, software that produces video almost always uses a Codec, which is a compression algorithm that can be proprietary. In some cases, the original digital recording must be played utilizing the specific manufacturer's software or with a compatible Codec. Agencies should consider purchasing solutions that retain the original format but also allow for a more standard format for each digital evidence item that allows for easier evidence review and management.

There are numerous types of digital video and audio recording devices with a variety of methods of exporting these files. Some will have CD/DVD writing capabilities, some use USB for output, and some, although digital, may only have analog outputs. The collection and forensic analysis of video evidence should be completed by someone who has proper training, tools, and certifications. This will ensure that when the video is being viewed, it is being seen in its original format and is not producing false speeds, images, and artifacts.

Vetting

Introduction
As with collection, vetting is primarily an issue for law enforcement agencies, however, courts and prosecutors also have a vetting role.

The three goals of the vetting process are to:

1. Confirm if the evidence is germane to the case
2. Confirm the integrity of the evidence and
3. Confirm the usability of the data (can it be played and/or converted).

Policy and Technical Considerations
To state that a piece of DME is authentic is different from pronouncing it "true" or "accurate". Discussions about authenticity center on questions of data integrity, to be determined from the source device as the evidence moves through the judicial process.

Fortunately, in one respect, maintaining the authenticity of evidence is getting easier for large classes of media evidence due to improving technology and vendors are including features in their software solutions that guarantee authenticity. Most software solutions available to law enforcement offer features such as automatic hashing of files, audit trails, and secure role-based access. Regardless, agencies need to have the ability to ensure and demonstrate that:

- No changes can be made to evidence that will ultimately be relied on in court, or if necessary changes are made (redactions, filtering, reformatting, etc.) there is a way back to the source file.
- Any person accessing the evidence is explicitly authorized and able to explain the reasons for all and every access request.
- There is an auditable trail that documents all interactions with the evidence with a standard that allows an independent party to later duplicate the process and achieve identical results.

Although ensuring the authenticity of DME from core tools such as dash cams, BWC, and closed-circuit television (CCTV) is getting easier, the huge growth of evidence being submitted from the general public and business users (including from bystander cell phones and private security cameras), means that overall the problem of assuring authenticity is potentially more challenging and certainly becoming more time-consuming.

Dissemination

Introduction

Dissemination of DME raises some unique challenges in the criminal justice system. In previous sections, the LEITTF reviewed the various challenges faced by law enforcement in collecting, vetting, and securing the captured evidence. Unless that evidence can be shared securely through the prosecution process it is effectively useless. The core problem is that at each stage of the evidence lifecycle, different groups of users require access to digital evidence from prosecutors, defenders, judges, court staff, and potentially appellate courts. At every stage, evidence is utilized in different ways by users who have different budgets and technical capabilities, obligations, and professional standards.

Policy Considerations

The diverse array of evidence stakeholders in the criminal justice process includes, but is not limited to:

- Investigators
- Prosecutors
- Judges
- Specialty Courts
- Defense Attorneys
- Clerks
- Court Staff
- Corrections
- Court IT Staff
- Evidence Technicians

In support of this broad spectrum of stakeholders, it is important to consider the use cases and requirements specific to DME. The table below outlines some of the key differences between a sample of stakeholder groups as it relates to dissemination.

	Law Enforcement	District Attorney	Public Defender	Court	Appellate Court
Use Case	Need to capture evidence quickly and efficiently from many sources. Need to review and redact quickly and efficiently.	Need to see police evidence quickly to evaluate and assemble a case.	Need to understand the prosecution's case and type of evidence. Must know about exculpatory evidence.	Need to see the evidence that the prosecution and defense seek to submit.	Needs to see what was allowed by the lower court and what the jury viewed.
Critical Requirements	Simple and secure collection tools and processes. Secure auditable storage. Efficient tools for extraction, conversion, and redaction. Robust, easy-to-use connections to prosecution systems.	Robust secure connections to multiple police departments. Forensic working copies of the evidence so that clear accountability and separation is maintained.	Visibility to all evidence. Easy access to forensic working copies of material, including originals on request.	Systems to allow evidence display in court, to remote witnesses, and to juries in the deliberation room.	Systems to allow playback in court and remote viewing.
Further Considerations	Software tools that allow for editing and redaction in situations where DME is allowed to be released to the public.	Software tools that allow for editing and redaction in situations where DME is allowed to be released to the public.	N/A	N/A	N/A

Additionally, DME is often a public record, and the public and press have a right to access the data, so their needs must be considered as well. Public access is often provided through a FOIA request and often requires significant redaction.

Technical Considerations

In addition to the policy considerations impacting the dissemination of DME, there also exist technical considerations as well. These technical considerations are intended to provoke discussions within the criminal justice agencies in jurisdictions attempting to address DME challenges as a whole.

- Source and Format Variety – Consider space allocation to support multiple copies of the DME. Evaluate the best option for an agency considering the systems in use by other agencies in the overall workflow. Leverage applications and storage solutions that support the larger business processes in the criminal justice system.
- Centralized or Decentralized – Centralized applications can mitigate security risks and allow for more cost-effective options. Additionally, centralized applications can limit effectiveness for the broader community because the goal is "one size fits all". Decentralized solutions can allow support for a variety of use cases unique to the various agencies in the criminal justice system. However, a decentralized solution can increase security vulnerabilities by opening up additional opportunities for cyber threats.
- Storage Volume – Inefficient storage software is the primary driver for higher storage costs. Agencies should evaluate solutions that transform software-defined storage into an enterprise storage platform.
- Audit/Log - NIST defines a security audit as: "A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports, and/or backward from records and reports to their component source transactions."[5] Audit logging and governance for viewing, modifying, and disseminating DME is crucial to the success of the overall solution.

There is now a seemingly endless list of sources for digital evidence, including BWC, cell phones, video recordings, audio files, and digital images. If the problems seem challenging for a single law enforcement body, imagine the problem for a prosecutor supporting multiple local and federal agencies. The prosecutor is responsible for supporting each agency's DME policies, which may have been implemented with varying degrees of operational and technical sophistication.

In many cases, individual software solutions for the storage and dissemination of DME may rely on proprietary storage formats. Several software solutions include tools that allow thousands of proprietary sources to be converted to standard file formats. Conversion to a standard format does not resolve Chain of Custody issues for the source file; however, conversion does bring advantages in terms of time-saving, reduced systems complexity, and reduced storage costs throughout the criminal justice system.

 5 – https://csrc.nist.gov/glossary/term/Security_Audit_Trail

Overarching Processes

Management

Introduction
Management is an issue for all the users along the evidence management lifecycle, including law enforcement, prosecutors, defense attorneys, courts, and other interested parties. Each of these users will share some of the same concerns, yet each will have unique challenges related to their role in the lifecycle. All stakeholders who interact with digital evidence must address storage, security, and virus protection concerns in the course of performing their respective responsibilities.

Technical Considerations
Since most DME originates from tools added to their daily routines, law enforcement agencies were the first to experience the avalanche of digital evidence files. The rapid rise of dash cams, body cams, surveillance video, and other gathered video along with the files extracted from phones and laptops was immediately felt by officers and agencies having to manage, organize, and review all that content. As the entry point for all digital evidence, law enforcement will have the largest burden of volume since they collect or receive everything related to an incident.

Furthermore, the prosecutors face a daunting challenge concerning the volume of data to review. They are often dealing with statutory time frames for charging decisions, so they have a limited timeframe to review the submitted digital evidence and make that decision. This becomes a staffing challenge since human intervention is required to examine the content and make that determination on how it proceeds.

The next big challenge for law enforcement is how to provide that volume of content over to the prosecutor for charging. Moving these files via disks, USB drives, and network drives was initially the answer and still is in many jurisdictions. With the current volume and rate of growth of these files, those methods are not secure, inefficient, not timely, and unwieldy. Some law enforcement agencies have cloud solutions included with their video capture hardware that can easily share files with other partners. However, the sharing of files can create Chain of Custody concerns. There is often a question among different agencies as to how to manage digital evidence storage. Should the agency rely on the original copy as captured by the law enforcement agency, or should individual users create and maintain a personal digital evidence repository with another copy for their purposes?

Prosecutors have the additional challenge of providing content over to a partner in the process since they have a responsibility to disclose all files quickly and fully to the defense attorney for the case. While this is often a "share all" requirement, there is still consideration to not move certain types of sensitive or sealed content to a cloud portal. In sharing the files with defense attorneys, the prosecutor must also ensure that the content can be viewed using commonly available technology.

When a case is going to trial, there is an additional level of management related to case preparation, authentication of digital files as well as admissibility concerns. As a case proceeds, there is still a high volume of organization required to manage the volume of digital evidence so attorneys can easily get to the needed files and identify the high-value content. For cases that proceed to trial, the courts will then have some volume of files they may also need to store post-disposition and for appeals. The need to securely share evidence with a jury must also be considered. While court volume is much lower and more controlled, they will increasingly face similar issues.

Finally, the cost of this volume of digital evidence storage cannot be understated. Stakeholders must first determine if they are going to pursue cloud-based or on-site storage. For both options, the considerations need to include back-ups, server and software maintenance, failover and failback procedures, security, and regulatory compliance. If all the stakeholders that play a role in the lifecycle of digital evidence agree on a solution, there are gains in sharing a single software application or platform to manage DME. This is often a challenge for partners with different purchasing rules, processes, and goals.

Compatibility and Consistency of File Formats

One file management issue most challenging for prosecutors but also felt at some level by all agencies is the wide variety of digital evidence file types. With multiple law enforcement submitting different types and volumes of evidence in a given case, prosecutors must find ways to organize and review almost every type of document, video, and audio that can be produced. Adding to this are the proprietary formats created by surveillance and video providers that will likely continue to grow as new vendors enter the market. The good news is special tools are available and evolving to improve the conversion and playback of most DME files.

Video and audio files are the biggest challenge since they have the widest variety of formats and are often the largest files related to a case. Along each step in the lifecycle of a case, there is a user who must easily be able to review the files and identify the portions of the file that are key to their respective need. For law enforcement, that may be a detailed and careful viewing to identify a person or find additional information. Prosecutors must quickly view every type of file they receive to make a charging decision. For cases going to court, both prosecutors and defense attorneys often must redact and reduce video and audio files, so they are consumable in a hearing or trial. Courts may be responsible for presenting video and audio files in a courtroom so the type of files they can manage is critical. Taking this wide variety of files and making them easily consumable takes time and is costly.

Compatibility problems are often felt in the transition between agencies: from law enforcement agency to prosecutor, prosecutor to defense attorney, and both attorneys into court. It is critical that systems between each agency can send and receive all types of files without any modification of the files or conversion of the file type. The integrity of the digital evidence depends on this transfer.

Retention Rules

Establishing retention management policies and following them is critical in any DME management system. Each agency type may have unique policies and guidelines, and some agencies may have retention rules or policies in place but violate them when they decide to just keep everything. The long-term cost of this practice can become burdensome when the storage cost of active cases alone is high. If agencies are sharing a copy for storage, additional business rules are needed to determine how the policies merge. In the prosecutor and court domain, cases that have gone to trial may have a longer life and stricter rules regarding retention. There should be some minimum amount of time that all files are kept and beyond that minimum, guidelines may be established based on the type of case.

When evidence requires expungement, often it's necessary to notify involved parties. When the files are older, tracking down those individuals can be a challenging task.

Tracking
As any evidence file moves through the lifecycle from law enforcement to prosecutor to defense attorney to court, each agency should ensure there is a thorough tracking mechanism that records every action on that file with, at minimum, the date, time, and user. This is necessary to prove the Chain of Custody, to maintain the integrity of the file, and to prove that discovery requirements were followed. This means stakeholders must be able to track a file as it moves between separate agencies to its final destination. See the Chain of Custody section below for additional details regarding Chain of Custody considerations.

The management process often requires some editing or modification of files, such as conversion for viewing, redaction, OCR, and Bates numbering. It's important that any process that needs to modify a file do so to a new version of the file to preserve the integrity of the original. The audit trail of any original file should prove it has not been manipulated, as it may be critical if the file is used in a trial.

Budget
Embedded in all the above challenges are the significant costs to each agency to store the files, acquire the tools to organize, view, and share files, and maintain a staff to perform all that work. If agencies can collaborate on ownership of files, it is possible to reduce redundant storage. That currently presents a challenge since each of the agencies along the process has its policies, processes, and sources of funding. It's difficult to align those without a significant effort because multiple agencies and branches of government are involved.

Some of the issues described above have a direct impact on the cost of managing digital evidence. Converting file formats to be easily viewable means storing an additional copy of often very large files. A lack of retention rules results in keeping all files, including additional versions created for editing across all cases resulting in continuously growing storage needs. DME management software must provide multiple methods of reducing costs inherent in the management process. Additionally, agencies need to implement processes and procedures that take advantage of cost-saving measures provided in their software.

Chain of Custody

Introduction
Participants in the criminal justice system face far more complex challenges than many of their counterparts in the private sector. For most businesses in the private sector, it is possible to create a defensible boundary for security purposes. In the criminal justice sector, the data can move between different agencies. This reality should cause Information Security Officers to ask, "How can we ensure confidentiality, integrity, and availability of data within our systems, but also ensure the same for data as it passes across the boundaries to partner or third-party systems?"

Chain of Custody refers to the documentation that establishes a record of the control, transfer, and disposition of evidence in a criminal case. Evidence in a court of law may include DNA samples, photographs, documents, personal property, or bodily fluids that were taken from a subject or discovered at the scene of a crime.

Evidence presented in court must be the same evidence that was recovered during the investigation and the prosecution must show the court that the evidence was handled properly and was not contaminated or tampered with. If the prosecution cannot prove to the court that the evidence was properly handled, the evidence can be challenged and potentially excluded from being used at the trial. Because criminal prosecutions rely on evidence gathered by law enforcement, prosecutors must establish the Chain of Custody for each item of evidence and that the requirements of the Chain of Custody policy are met.

Policy Concerns

Proving the Chain of Custody can be difficult. If law enforcement does not manage evidence following policy, the Chain of Custody can be successfully challenged in a criminal case. If the judge finds that certain evidence is not admissible, the prosecutor might not have enough evidence to proceed with a case.

Chain of Custody issues are particularly important in cases involving drugs, guns, or samples that have been tested for the presence of drugs or alcohol to prove intoxication. To prove the Chain of Custody, documentary and testimonial evidence have to be presented to lay a foundation to establish that the evidence under consideration at trial is the same item that was in the possession of the defendant before his/her arrest before it is accepted by the court. DME is no exception to this process, and while materially different, the same procedural challenge can be made to any digital evidence sought to be introduced in court.

In a typical case, a police officer will collect evidence (both physical and digital) at the crime scene and transfer custody of the evidence to a forensic technician. In the case of physical evidence, the technician analyzes the evidence, for example, by testing a blood sample for the presence of alcohol or other intoxicating drugs, collecting fingerprints, or verifying that a substance collected at the scene is, in fact, an illegal drug. The forensic technician must document any tests that were performed on the evidence. When they have finished testing the evidence, they turn it over to an evidence clerk, who stores the evidence until it is needed for another test or to be presented at trial. To prove the Chain of Custody at trial, law enforcement must be able to identify, at all times in the Chain of Custody, a particular person who is in control of a piece of evidence. This is done through an evidence log.

An evidence log for physical evidence includes the date and time the evidence was collected, the name of the investigator, the location where the evidence was collected, the reason the evidence was collected, relevant serial numbers, a description of the evidence, and the method that was used to collect the evidence. The evidence log should also include the signatures of the people who possessed the evidence, the date and time the evidence was transferred, how the evidence was transferred, and the security conditions while the evidence was being handled or stored.

There are further complications arising from the need to modify data formats as data moves between systems (e.g. when video is encoded at a lower resolution or in a different format to meet cost or functional targets. If modification must occur, should it occur in the source system (raising cost) or be modified by the recipient? If modified, should the source and recipient both keep records and how can originals be retrieved easily when a need arises?

Concerning DME, the logging requirements are substantially the same. Any digital evidence that has been viewed, redacted, or shared must be logged with the same level of detail as physical evidence. Further, because digital evidence is more prone to accidental modification, it is critical to enact procedures that require, at a minimum, the following:

- The Original – The evidence as collected.
- Forensic Copy – A bit-for-bit mirror copy performed in a forensically sound manner.
- Forensic Working Copies – A copy of a forensic copy. This process can be repeated as necessary to perform analysis, distribution, redaction, etc.

Any time evidence is examined (physical or digital), the examiner must list everyone who came in contact with the evidence and all interactions with the evidence.

Conclusion

While the need to manage DME is growing and changing, the underlying processes of evidence management remain the same: Collect, Vet, and Disseminate. Underlying it all is the need to provide both the necessary security and privacy protection both citizens and the government strongly desire. The LEITTF has attempted to describe the major considerations agencies should evaluate as they work with their criminal justice partners to support the increasing demand our digital world places on their public safety mission, and all the critical steps within that responsibility.

The factors and concerns presented herein should be used as a baseline for DME technology usage and related policies and procedures. This document is by no means all-inclusive nor ever "complete" – the concepts within it must be constantly reevaluated and refined to match the rapid pace of technological development and the courts' acceptance of its capabilities. The public's appetite for law enforcement access and usage of digital evidence must also be constantly gauged, especially considering the potential intrusions into the lives of people potentially unrelated to crime investigations.

Finally, the financial implications to agency budgets must also be weighed against all things that a properly operated DME system requires. Participating in a secure, efficient, and trusted DME environment is a significant cost to agencies, and taking shortcuts can be more costly and time-consuming in the long run. This document can be used by agencies to help estimate costs by knowing what elements of DME system participation are necessary, thereby assisting with financial forecasting.

Agencies should continue to discuss challenges and successes with peers in other jurisdictions to learn how neighboring agencies are conducting DME environments, and what gaps and efficiencies are being discovered. Digital evidence is a rapidly developing challenge for the entire justice system, and the only thing for certain is that it will be part of the way law enforcement conducts business for the foreseeable future. The LEITTF hopes this document helps ease some of the uncertainty ahead and assists you in ensuring digital evidence is not simply less troublesome, but the strongest element of your public safety mission.