

DIGITAL EVIDENCE

UNCOVER THE IDEAL DIGITAL EVIDENCE
MANAGEMENT SYSTEM (DEMS) FOR YOUR AGENCY:
A IN-DEPTH GUIDE

WHAT TO LOOK FOR IN A DEMS

Cloud and on-premise both have advantages. Learn the truth behind this and more.

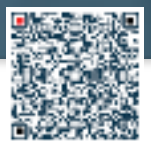
COST VS REWARD OF INVESTMENT

Cost alone doesn't determine the best choice. ROI, features, and support matter more.

THE FUTURE, WHAT TO EXPECT

Exploring AI and other upcoming advancements to empower Law Enforcement.

FileOnQ



SCAN TO LEARN
MORE AT
FILEONQ.COM

INTRODUCTION



Year after year, police departments struggle to manage exponentially more digital evidence. Inexpensive digital CCTV systems are now commonplace in communities while crime scene photos, recorded interviews, and citizen shared digital evidence are also more frequently being handled by officers and detectives. Adding to this, many agencies have adopted in-car and body worn camera (BWC) systems ensuring high resolution video must be stored and managed for even minor police calls.

The CCTV market has hit an inflection point where surveillance video systems are now: (1) affordable, (2) capture high quality video, and (3) easy to install and configure. Cloud based systems (such as Blink, Arlo, and Ring) can be installed in just a few minutes by virtually anyone with a wireless internet connection. Almost no technical skills are needed. This has led to a surge in CCTV cameras being installed in neighborhoods throughout the United States.

Departments simply can't ignore digital evidence. Police administrators have a responsibility to provide officers with basic digital evidence competency training, particularly in recovering and reviewing surveillance video. Agencies must also have a system in place to securely collect, manage, review, and share digital evidence utilizing best practices and adhering to laws and regulations within their jurisdiction.

The stakes are high. Lost or mishandled digital evidence calls into question an agency's credibility while jeopardizing important cases. A Digital Evidence Management System (DEMS) is the virtual command post for managing all the digital evidence collected by officers. A DEMS, along with training and department policy utilizing best practices ensures agencies properly collect and maintain their case evidence.

ON-PREMISES OR SAAS DEPLOYMENT OPTIONS

1

There is a significant risk of storing just one copy of any file. If the storage system crashes or specific files become corrupt, it may be necessary to utilize backup copies. Therefore, it is best practice to have at least two copies stored in different geographic locations and storage systems. For example, digital evidence could be stored locally (on-premises) with a backup in the cloud. Storage redundancy ensures backup copies of digital evidence always exist.

A DEMS should be able to store digital evidence locally (on-premises), in the cloud, or both. Having both storage options allows agencies to push older evidence into less expensive Azure storage while leaving recent case evidence on a local server that offers much faster access times.

Some evidence storage may be required to comply with CJIS security policy and follow local regulations. Federal agencies may require FedRAMP compliance for cloud-based software solutions.

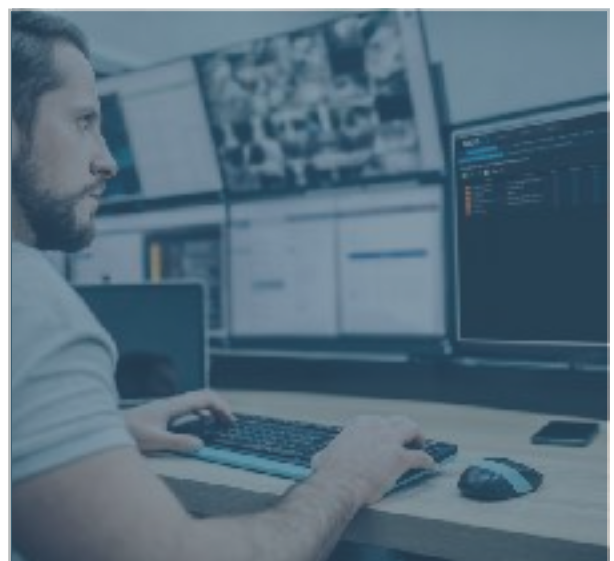
✓ **DigitalOnQ offers flexible deployment options** including on-premises (installed on a NAS or local server) or Software as a Service (SaaS) utilizing Azure for US Government secure cloud storage. DigitalOnQ meets CJIS and FedRAMP strict requirements for security and access control.

SECURE AND COMPLIANT

2

Access to digital evidence is designated within the DEMS at individual and group levels. Personnel are granted or denied access to specific case types based on their role in the police department. For example, patrol officers may be given general access to digital evidence in the system, but excluded from accessing sensitive special assault evidence, while detectives investigating special assault cases would be granted full access. Individual and group level access privileges are configured by the agency and can be updated or modified at any time.

✓ **DigitalOnQ includes granular user and group level permissions** and follows best practices for handling and storing digital evidence.



A MODERN DEMS SHOULD ADHERE TO AND ENSURE THESE BEST PRACTICES

1

EVIDENCE COLLECTION: Officers and investigators capture digital photographs, collect CCTV video, and other media in the field. Citizens also share evidence. Forensic specialists extract digital evidence from phones and other devices.

2

EVIDENCE INVESTIGATION: Digital evidence collected by officers, investigators, and forensic specialists are then stored in a DEMS. The system must be secure and protect the digital evidence from changes or unauthorized access.

3

EVIDENCE CASE MANAGEMENT: After digital evidence has been collected and stored, it must be accessible. The DEMS must track chain-of-custody and user access while allowing investigators to review evidence in their cases.

4

EVIDENCE SHARING: As an investigation unfolds, digital evidence may need to be shared with other specialists, investigators, and prosecutors. It may also be shared with defense attorneys and outside experts if the case ends up in court.

5

EVIDENCE STORAGE & ARCHIVING: In most jurisdictions, digital evidence must be stored for several years after a case has been adjudicated. Even digital evidence in minor cases will usually be stored for some extended period of time.

6

EVIDENCE PURGING: Most jurisdictions have retention laws governing how long evidence can be retained and when it must be purged. DEMS can track evidence retention and alert administrators when it's time to purge evidence.

STORAGE AGNOSTIC AND SCALABLE

3

The DEMS you choose should be flexible and integrate with a wide variety of storage solutions. For example, a small police department may elect to store their evidence internally on a Synology NAS while larger departments may opt to utilize more expensive hybrid on-premises/cloud solutions. The DEMS should also be scalable, allowing departments to increase their storage capacity as necessary or daisy chain multiple storage options together. Be cautious of vendors who suggest locking into a proprietary storage solution as the cost of maintaining the DEMS will likely become progressively more expensive each year. In addition, it can be challenging and costly to migrate large amounts of digital evidence to another solution after being locked into a proprietary system.

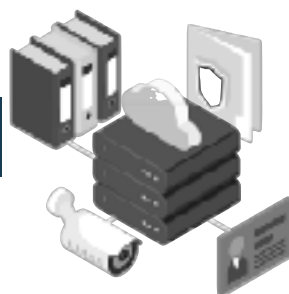
✓ **DigitalOnQ is storage agnostic and can be configured** to store digital evidence on virtually any secure storage container including a NAS, on-premises server, or offsite utilizing Azure for US Government encrypted cloud storage.

CLOUD HOSTED



OR

ON-PREMISE



INTEGRATES WITH BWC AND OTHER SYSTEMS

4

Body Worn Camera (BWC) systems are not DEMS solutions. As police departments adopt BWCs, it's becoming increasingly important for BWC and DEMS solutions to work together. Integration between systems allows investigators to bring together all digital evidence associated with a case for review.

For example, while investigating a homicide, an agency may have 10 or more BWC videos from patrol officers who assisted or were on scene. There may also be digital photographs, surveillance video from multiple locations near the incident, audio and video recorded interviews, as well as other digital evidence. A flexible DEMS can handle all this digital evidence in one place. It should also be device agnostic, meaning you're not required to use specific hardware. By using a centrally managed, non-proprietary DEMS, agencies can avoid having system silos or redundant solutions.

✓ **Are your officers forced to work between multiple evidence systems?**

DigitalOnQ is designed to be the digital evidence management system of record and single source of truth. We've partnered with Axon, Motorola, and other companies to integrate with DigitalOnQ. Bringing together critical digital evidence systems via seamless integration eliminates the need for officers to log into multiple systems and ensures all case evidence is shared with prosecutors and other stakeholders.

SUPPORT FOR MIGRATION OF YOUR DIGITAL EVIDENCE

5

Ongoing support is critical to successfully deploying a DEMS. Without a team of experienced installers and knowledgeable subject matter experts, you may be left managing your evidence alone or forced to pay high support fees to get help. The DEMS solution you choose should include a team dedicated to migrating your existing digital evidence into the new DEMS and providing ongoing technical and professional support.

✔ **FileOnQ's deployment team has many years of experience migrating existing digital evidence** (from other systems) into DigitalOnQ. After DigitalOnQ is installed, configured, and deployed, our team can migrate older digital evidence into DigitalOnQ.

DESKTOP APPLICATION, WEB, AND MOBILE APP FLEXIBILITY

6

Many DEMS solutions simply offer web access to digital evidence, which may offer limited functionality. A comprehensive DEMS solution should offer a feature-rich desktop application, web access, and mobile applications.

Police administrators and detectives may use the desktop application to take advantage of advanced features while patrol officers may elect to upload digital evidence throughout their shifts using the mobile application. Officers can upload digital photos directly from the scene or quickly review surveillance video collected by another officer prior to contacting a high-risk suspects in the field. Empowering officers with a powerful mobile app improves officer awareness and safety in the field while saving time.

Web access to your DEMS allows virtually anyone on the network to upload and review digital evidence (provided they are authorized users). In addition, since web access doesn't require special software to be installed and maintained on every workstation, this significantly reduces the amount of time an organization's technology department must spend supporting desktop systems having the DEMS application installed.

✔ **Officers can access DigitalOnQ via a feature rich desktop application, DigitalOnQ Web, or DigitalOnQ Mobile** (supporting Apple iOS and Android). Oftentimes officers encounter fast-moving investigations requiring quick action. With DigitalOnQ Mobile, officers can search for critical case video, persons-of-interest images, and other important digital evidence while in the field.

CHAIN-OF-CUSTODY EVIDENCE TRACKING

7

As with physical evidence, digital evidence should be tracked in detail throughout its lifecycle. One of the most basic functions of a DEMS is to track chain-of-custody.

A DEMS catalogs every person who has accessed individual files and itemizes the date and time case evidence has been viewed, downloaded, printed, or shared. The system should also include comprehensive reporting tools allowing investigators to quickly print chain-of-custody reports detailing every interaction beginning when the digital evidence was first ingested into the system. Not only does this ensure evidence integrity for court, but it also gives police administrators tools to discover how digital evidence may have been inappropriately viewed or shared outside the department.

For example, if a sensitive video from a case was posted on social media, administrators can produce a report detailing every person who interacted with the video and other digital evidence in the DEMS. This encourages department-wide transparency and accountability.

✓ **DigitalOnQ tracks interactions with every file in the system in real time** including viewing, printing, sharing, downloading, annotating, annotation changes, editing, and reporting. DigitalOnQ's detailed chain-of-custody tracking system allows administrators and prosecutors to discover how digital evidence is handled.

IMAGE AND VIDEO ENHANCEMENT OPTIONS

8

Many times, investigators need to quickly prepare images or short surveillance video clips for media release to help identify or locate a suspect. The DEMS you choose should offer tools for enhancing images and video allowing investigators to isolate a person or vehicle of interest, add arrows and other callouts, adjust brightness and contrast, apply a case number, and include other critical case information. Enhancements should be applied to derivative copies and never change the original evidence.

✓ **Using DigitalOnQ's enhance tool, investigators can easily prepare images for media release** by cropping a person of interest, rotating, adjusting brightness, adding a case number, and agency patch. DigitalOnQ enhance tools include brightness, contrast, hue, saturation, exposure, opacity, blur, as well as arrows, shapes, text, and image overlays. DigitalOnQ creates a copy and always preserves the original.



Filters

ORIGINAL DIGITAL EVIDENCE NEVER CHANGES

9

Defense attorneys oftentimes challenge the integrity of digital evidence introduced in court. It usually starts with a question from defense, "Detective, how do we know this is the same surveillance video you recovered two years ago, and it hasn't been altered in some way?" A question like this can be an effective defense strategy for excluding critical evidence during a trial for agencies without a DEMS.

File hashing is used to track evidence integrity.

A DEMS produces a hash of every digital file as they're uploaded. A hash is a unique hexadecimal string created by a widely researched mathematic algorithm. Since hashes are effectively one-of-a-kind, they can be thought of as digital fingerprints. For example, even though two images appear to be the same, if the hashes are different, we know something between the two files has changed. Simply changing a single pixel in one of the images will generate a different hash.

Hashing traditionally occurs as digital evidence is uploaded or ingested into the system. Your DEMS should be able to quickly generate a hash report for all of the digital evidence in a case. This report can be provided to the court and help prove the integrity of any files in question.

✓ **DigitalOnQ applies a SHA-256 hash to every file** as they are uploaded. This allows investigators to quickly verify that critical evidence hasn't changed, and prosecutors prove evidence integrity in court.

IF THE HASH VALUES MATCH,
THE TWO FILES ARE THE SAME.



bdbf 6150 9966 8893
328d 1024 1f0b edd6

bdbf 6150 9966 8893
328d 1024 1f0b edd6

LAW ENFORCEMENT EVIDENCE SHARING

10

Sharing digital evidence securely with prosecutors, outside agencies, and other critical stakeholders is a challenge for many police departments. This struggle is compounded as digital evidence grows. Surveillance video that once was just a few megabytes may now be many gigabytes. Copying digital evidence onto discs or thumb drives can be extremely time-consuming. Not only that, sharing evidence on loose media is insecure. Discs, thumb drives, and portable hard drives can be easily misplaced or mishandled and end up in the wrong hands.

Sharing critical digital evidence should be secure, uncomplicated, and straightforward. With a DEMS, investigators can securely share an entire case with a prosecutor as a direct download. Most DEMS allow shared evidence to be password protected and limited so case files can only be downloaded during a specific period before expiring and removed from the shared server. In addition, chain-of-custody is tracked so the agency knows with whom and when digital evidence was shared. Prosecutors appreciate being able to quickly access case evidence as it streamlines the discovery process.

 **With DigitalOnQ, officers and investigators can securely share digital evidence** with stakeholders in just a few seconds. Shared evidence is accessible for a limited time and can be revoked if necessary. Information about the date, time, and person shared with are tracked.

CITIZEN EVIDENCE SHARING


11

Patrol officers face the challenge of handling digital evidence shared by citizens. DEMS solutions now have citizen sharing features that make acquiring and storing evidence quick and efficient.

Citizens commonly share smartphone images and videos as evidence. However, officers also come across text messages, chats, emails, social media screenshots, and other media. Without a DEMS, officers rely on citizens to share evidence as email attachments or try to save it themselves, which is frustrating and time-consuming.

Email attachments and cloud services like Dropbox present security risks and potential public disclosure issues. Videos or images sent to officers may also be reduced in size and quality on mobile devices.

Prioritizing citizen sharing capabilities in a DEMS solution is crucial. Officers can request citizens to directly upload evidence to the police department's evidence server from their smartphone via text message or email. The DEMS system manages the transaction, saving time and frustration and ensuring a complete chain of custody.

 **DigitalOnQ's Citizen Share mobile app enables investigators to request digital evidence from involved citizens** in the field. Officers enter case details, sender's information, and the request is sent. Victims or witnesses can securely send selected digital files back to the officer using their phone or computer.

A DEMS SHOULD MANAGE ALL FILE TYPES

12

Officers and detectives encounter a wide variety of proprietary and non-proprietary file formats including digital images, video, audio files, documents, text messages, and emails. In some critical cases, detectives may generate proprietary crash data or unique computer and mobile forensic files stored in complex folder structures. Regardless of the file format or folder structure, all digital evidence generated in a case should be available to investigators and prosecutors in one place. A flexible DEMS solution can ingest and manage any file type while maintaining the original folder structure.

✓ **Officers and investigators can upload any file type into DigitalOnQ.** This includes non-proprietary and proprietary file formats such as digital forensic evidence. Most non-proprietary file formats can be reviewed or played directly within DigitalOnQ.

ADVANCED SEARCH AND GROUPING

13

As digital evidence is collected and uploaded in a case, investigators need search tools to quickly find and review the most important files. This is particularly crucial in serious, fast-moving cases.

Consider a homicide investigation involving suspects fleeing in a vehicle through several busy city blocks. There are businesses and homes with

CCTV systems along the escape route. Officers and detectives rapidly recover surveillance video from 10 locations hoping to develop a lead in the case; however, they know some of the video they recover may not have recorded the suspects. As they identify video clips of interest, they need to quickly separate and organize the most critical evidence in the case.

Some DEMS have comprehensive search and organizational functionality. This allows investigators to quickly find and separate the important evidence into virtual folders. For example, detectives may create folders containing surveillance video from specific locations and other folders containing still images of the suspects and getaway vehicles. Organizing digital evidence into virtual folders helps investigators, prosecutors, and other collaborators quickly locate the most important assets as a case is investigated and reviewed for charging.


✓ **DigitalOnQ includes a powerful search tool called Query Builder.** Query Builder allows officers, detectives, and police admin to build and save commonly used unique searches that can be reused over again. For example, a major crimes supervisor could create a query search for all digital evidence related to felony crimes uploaded in the last week. DigitalOnQ also has advanced sorting and group options to help investigators review 100s or 1000s of files in a case.

COMPREHENSIVE REVIEW MODE FOR INVESTIGATORS

14

After digital evidence has been uploaded, investigators need to be able to watch surveillance videos, review digital images, listen to audio files, and preview documents. Support for file review is fundamental to Digital Evidence Management Systems. Some DEMS allow investigators to review documents and other non-proprietary file types without having to download a copy to examine outside the system.

Review mode within a DEMS should be easy to use while providing important information about the files being viewed. The system should catalog the date, time, and users who have viewed, downloaded, printed, or shared the digital evidence being accessed. This becomes an audit record for chain-of-custody reporting.

 **Non-proprietary files can be reviewed directly within DigitalOnQ.** This includes most image, video, audio, and document file formats. As investigators are reviewing evidence in a case, they can also examine file metadata and audit logs connected to each file.

increasingly more digital evidence (images, videos, and other files) while also utilizing increased storage space (as files are getting progressively larger in size). To predict how much digital evidence storage an agency needs in the future, it must know how much is currently being stored as well as been ingested in previous years.

Some DEMS have comprehensive reporting features which can quickly determine how much digital evidence an agency has. A DEMS should be able to break down how much digital multimedia evidence was collected by week, month, and year and itemize the number of videos, images, documents, and other file types being stored. Comprehensive reporting tools allow police administrators to predict how much storage they will need in the future.

 **Investigators can generate a variety of critical reports** in DigitalOnQ including chain-of-custody, evidence hashing, outside sharing, user activity, image proof sheets, and more.

COMPREHENSIVE REPORTING TOOLS

15

As technology advances, digital multimedia continues to grow in size and quality. Most police departments discover they are collecting

ADVANCED RETENTION AND PURGING FEATURES

16

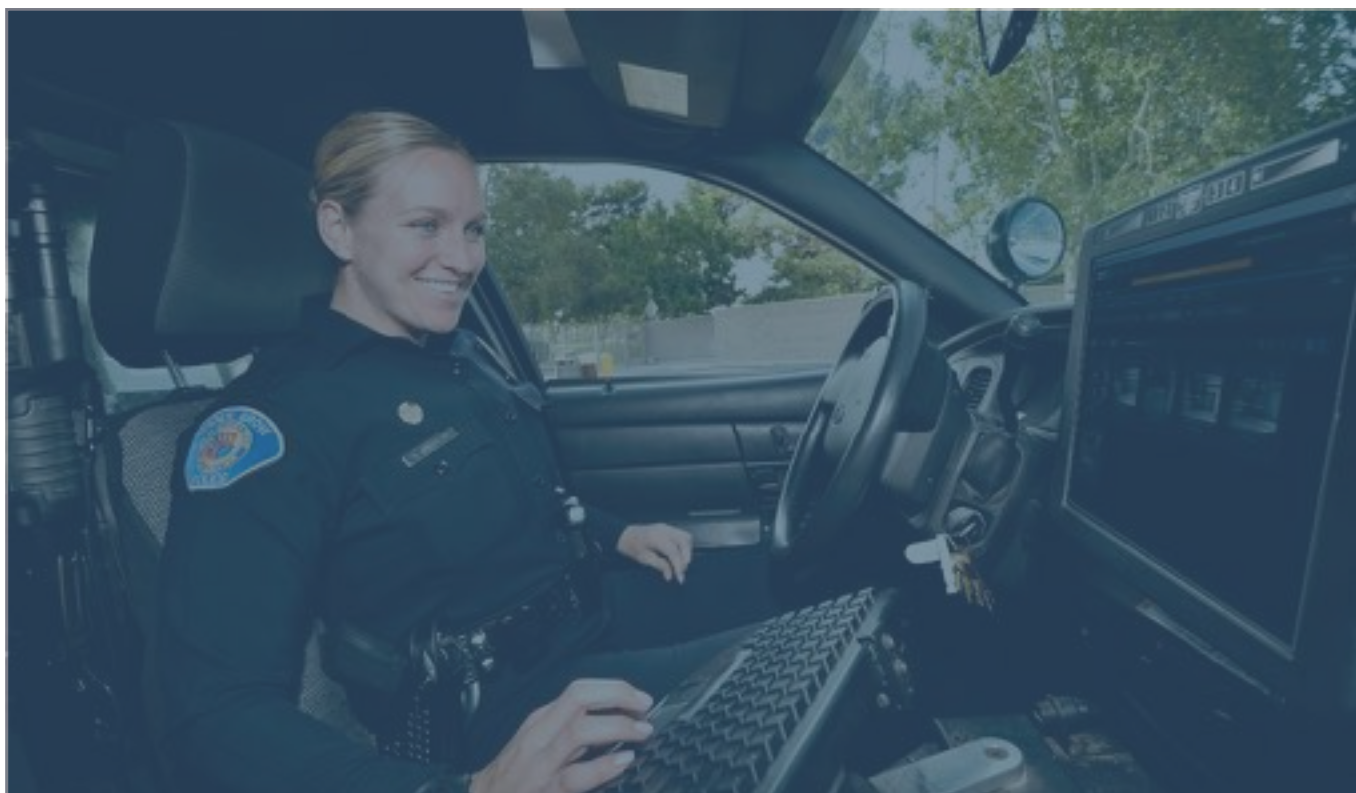
Digital evidence in cold or serious criminal cases are usually kept indefinitely, while evidence in many adjudicated cases will eventually need to be purged. Evidence retention is based on state and local guidelines and laws. Without a DEMS, agencies are left to comb through and purge digital evidence manually. Even for small agencies, this isn't practical. Purging digital evidence by hand is also risky as it is relatively easy to inadvertently delete the wrong folders or files.

Your DEMS should include evidence retention settings that can be set up to send reminders when digital evidence in a case is ready to be purged. Coordinate your DEMS retention settings with those of your physical evidence system, and your staff will always be alerted when it's time to purge all evidence in a case. Once it has been determined evidence in a case should be purged, the DEMS admin (or their designee) can initiate the purge and delete all the digital evidence associated with the closed case.

A DEMS can purge all the digital evidence in a case and the record of its existence or purge the digital evidence while retaining the record. Retaining the record allows records staff, evidence specialists, and investigators to search previously purged cases to see what digital evidence once existed while following local and state evidentiary retention guidelines.



DigitalOnQ includes an advanced retention system which can be configured to alert police administrators and supervisors when evidence may be eligible for purging. To prevent digital evidence from being deleted accidentally, several security checks must be completed by authorized administrators. Chain of custody and audit logs are retained for transparency. hasn't changed, and prosecutors prove evidence integrity in court.



WHAT TO EXPECT IN THE FUTURE FOR DEMS SOLUTIONS

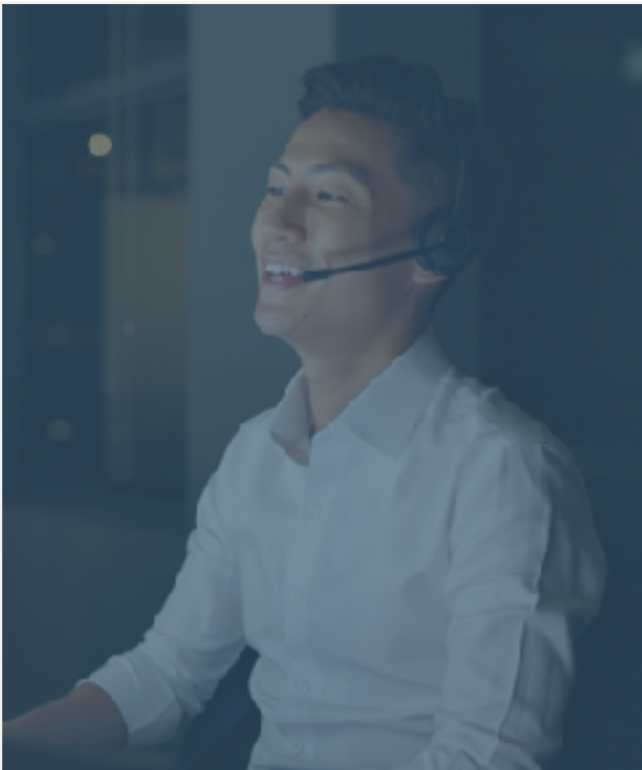
Digital Evidence Management Systems are quickly becoming more sophisticated by tapping into cloud computing and AI deep learning technology. By utilizing cloud computing resources, a DEMS can automate redaction tasks (blurring faces, license plates, and RMS screens). There are also a variety of video analytic applications being pursued which help investigators analyze long segments of video by quickly identifying persons, vehicles, or objects of interest in a specific location or aid in tracking persons or objects through a series of video segments.

Proprietary CCTV video playback continues to be an on-going challenge for many police departments. With thousands of proprietary surveillance video file formats, DEMS vendors are looking for ways to automatically convert tricky video files into a non-proprietary format so that they can be played directly within the DEMS. Comprehensive support for proprietary video playback directly within a DEMS can significantly shorten the time it takes investigators to locate suspects or vehicles of interest in a case.

ABOUT FILEONQ

FileOnQ offers a customizable [no-code software management solution](#) to criminal justice and law enforcement agencies. **Our team of consultants, with over 20 years of experience in various areas of the criminal justice system,** provides expert guidance.

We not only provide software but also offer high-quality training to assist agencies in policy development, accreditation preparation, evidence facility transition, and other specialized projects. Our support and training have been praised as exceptional by agencies, surpassing their expectations compared to other software companies. Additionally, we ensure a seamless installation and implementation process.



TALK TO AN EXPERT

Contact us if you would like to talk about digital evidence management best practices or learn more about how DigitalOnQ can help your agency. You can request a demo [here](#).

[Get Connected](#)

800.603.6802

RESOURCES

Finding a DEMS solution and adopting best practices for digital evidence handling can be overwhelming. It may be especially daunting if you manage a smaller agency and don't consider yourself or anyone in your organization very technical. That's ok! There are several resources available to get you pointed in the right direction.

ORGANIZATIONS AND STANDARDS

- SWGDE – [Scientific Working Group on Digital Evidence](#)
 - Develops and publishes guidance documents for handling digital evidence.
- IAI – [International Association for Identification](#)
 - Offers a forensic video certification.
- HTCIA – [High Technology Crime Investigation Association](#)
 - Non-profit organization for high tech training, education, and networking.
- NIST, OSAC Standards and Guidelines – [Organization of Scientific Area Committee](#)

Training

- Surveillance Video Recovery and Analysis Training:
- [LEVA – Law Enforcement Video Association](#)
 - LEVA is internationally recognized and widely considered the starting point for individuals new to video forensics. LEVA offers multi-tiered training and certification.
- [National Center for Media Forensics](#)
 - University of Colorado Denver offers training in audio, video, and image evidence collection, analysis, interpretation, and presentation.
- Digital Evidence Handling Training:
 - [NW3C](#) – White Collar Crime Center offers cybercrime, cybersecurity, and digital forensic course among many others.
 - Look for Basic Digital Forensic Analysis: Seizure (BDFA)



832 Industry Drive Seattle WA | 800.603.6802 |
<https://fileonq.com>