Introducing the future of digital forensics and evidence management

Building your edge-to-core-to-cloud digital forensics and evidence management platform for today and tomorrow

The breadth, leverage, and growth of digital evidence has increased exponentially over the past few years as more data is coming from devices such as computers, CCTV cameras, smartphones, body-worn video, and vehicle-based data.

The pervasiveness of this data is leading to significant advances in the protection of citizens and is dramatically changing how the law enforcement community approaches criminal investigations.

Indeed, the success of a criminal investigation depends on the thorough and accurate collection and analysis of evidence found at the crime scene. In recent years, the use of evidence management systems has become a major trend in forensic labs as they are regarded as essential tools helping forensic analysts work more efficiently to support the full evidence lifecycle from crime scene to the courtroom.

Digital and physical evidence used to be managed separately. In recent years, however, courts are recognizing both types of evidence equally, and both are prioritized equally regarding their chains of custody and evidence integrity.

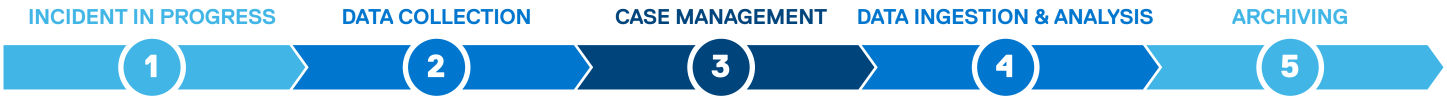
WHAT'S THE DIFFERENCE BETWEEN DIGITAL EVIDENCE AND DIGITAL FORENSICS?

DIGITAL EVIDENCE
is data stored or transmitted that may be relied on in court or can help law enforcement to maintain individuals in custody. It can include data on computer hard drives, smartphone footage, CCTV footage, emails, social media posts, and many other pieces of information.

DIGITAL FORENSICS
is the process of identifying, preserving, analyzing, and documenting digital evidence for use in criminal investigations.

MANAGING THE WORKFLOW WITH AN ENTERPRISE-INTEGRATED APPROACH

The digital forensics and evidence management workflow extends from the collection of data through to the presentation of conclusions and the archiving of the case. It can complement real-time situational data that police departments leverage to make better informed decisions during an incident. However, the centralizing factor is the provision for scalable, centralized storage.



Incident in Progress: As incidents occur, evidence data is created from a wide range of sources, including situational awareness data from sensors and cameras as well as physical and digital evidence and more traditional forms of evidence such as interview audio files and emergency call transcripts.

Data Collection: During the course of an investigation, digital evidence will be gathered for the ultimate objective of producing a conclusion such as a conviction.

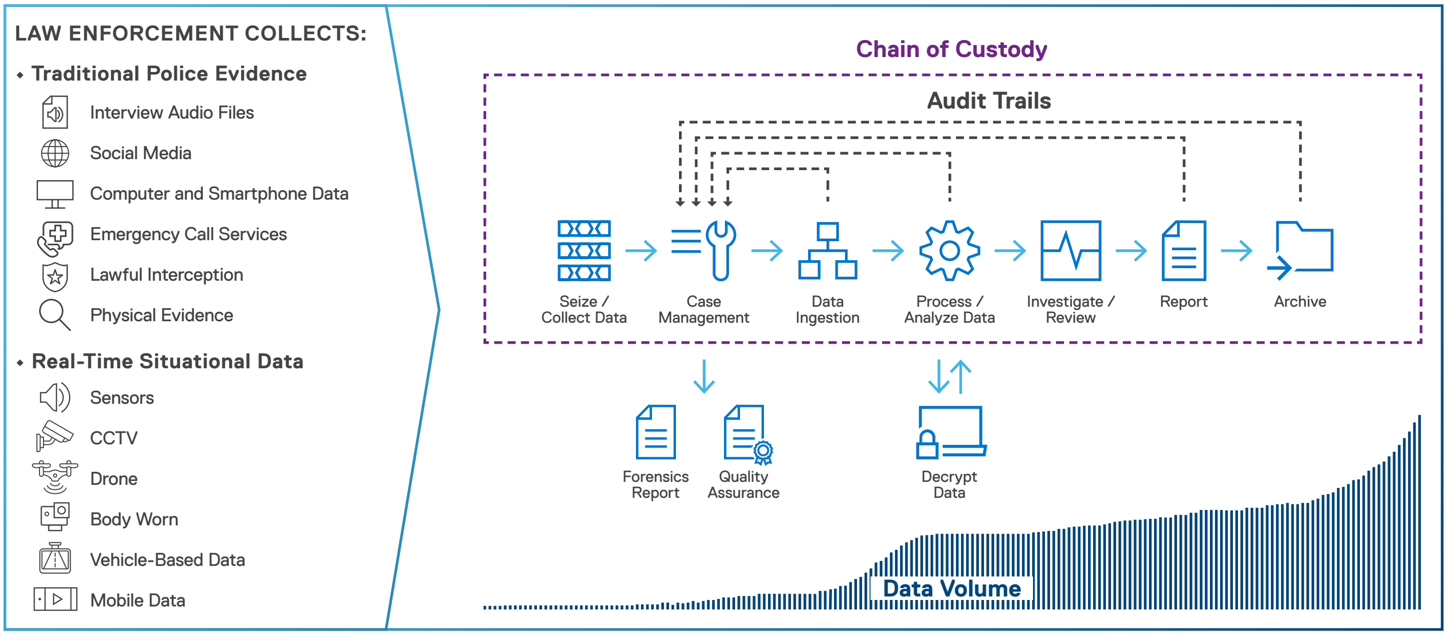
Case Management: The collected data is moved into a dedicated case file for tracking, assigning tasks, throughput, collaboration, reporting, and integration with other tools.

Data Ingestion & Analysis: A chain of custody must be preserved as data is uploaded, tagged, and prepared for processing and analysis. This may involve decryption if the data has been seized from a social platform where it is kept secure.

Archiving: Once digital evidence has been ingested, processed, and analyzed, it will need to be archived securely, so that it can be retrieved quickly and accurately when needed.

A CENTRALIZED PLATFORM FOR DIGITAL FORENSICS AND EVIDENCE MANAGEMENT

Simplifying and automating the digital evidence lifecycle with complete chain of custody and audit trails



Streamlining digital forensics and evidence management

Managing the rapidly expanding volume and variety of digital evidence at each stage of the workflow from data ingestion to analyzing to archiving can be complex, especially with most case data and applications currently being kept in siloed systems. For example, 94 percent of investigators face challenges with video evidence.[1] To help simplify and streamline investigator workflows, agencies need an enterprise-integrated approach that brings together the broad ecosystem of software and hardware, ranging from basic device management and multimedia file storage through to seamless integration with new and existing police and control room systems.

Dell Technologies can help simplify, consolidate, and streamline deployment of your digital evidence management ecosystem, with an architecture that is sized to respond to the growing need for processing and analyzing the data. By combining Dell Technologies lab-validated workloads for forensics, video and data analytics, hyperconverged and storage platforms, and industry-specific software in a scalable architecture, we deliver solutions for digital forensics and evidence management that work for your organization from day one. Together with our curated partner ecosystem, we provide the right solutions that are designed to meet the challenges of modern law enforcement and all of your use cases.

MODERNIZING YOUR DIGITAL FORENSICS AND EVIDENCE MANAGEMENT PLATFORM

Investigators, officers, prosecutors, and forensic analysts need to perform their jobs with expediency and accuracy. However, ensuring that evidence is properly collected, documented, packaged, and stored correctly is challenging from a technical, legal, and resource perspective.

To address these challenges, today's agencies require:

- **A centralized platform serving multiple uses:** Traditional systems for digital forensics and evidence management tend to be siloed by application, department, and often geographic location. Having access to information in a centralized repository avoids having to sift through multiple systems, both physical and digital. Centralization means time saved from not having to travel, reduction in overhead costs, and greater security. This allows law enforcement to benefit from the ability to run different tools on the same platform with the flexibility to access data sources when and where needed, enabling investigations to proceed more quickly. Evidence can also be accessed remotely if required, giving investigators the flexibility to upload and access critical evidence from the field. In addition, a centralized platform simplifies data ingestion, archiving, and backup so that they can be performed in parallel, further expediting workflows.

- **Security, compliance, governance, and chain of custody:** For evidence to be admissible in court, the chain of custody must be preserved and provable. Access to assets needs to be safeguarded while also providing flexible and granular user and asset security policies. The chain of custody should be preserved and recorded with full audit logs showing who has accessed a piece of evidence and any operations performed on it. This means that the original piece of evidence can be preserved for legal proceedings, increasing the need for the data to be accessible. A digital evidence management system must ensure proper governance and compliance in accordance with the laws and regulations of a given jurisdiction. An example would be data retention regulations, ISO standards, and practices such as the European Union's GDPR or the Criminal Justice Information System in the United States.

- **Migration of historical evidence:** Some cases may date back years or even decades, and the associated evidence must be preserved. As technologies become obsolete, data must remain accessible in an affordable fashion so that critical evidence is not lost as official support for associated devices ceases. Historical evidence ingested into the system must also remain compliant.
- **Future-proofed scalability:** The digital evidence system must be able to keep up with the constant expansion of storage needs and processing capacity. This ranges from the ability to add nodes to expanding storage to increasing networking as needs arise.
- **Analytics and automation:** Digital evidence can be stored in a single or multiple clouds, on-premise, or a mix of both. Having digital evidence, data, and video analytics all accessible within a secure multi-cloud or on-premise environment allows for scalability, advanced analytics, easy data sharing, and enhanced workflows. Footage, for example, can be directly outputted into the evidence system for more efficient allocation of investigations, police resources, and record keeping. Forensics platforms leveraging advanced analytics such as artificial intelligence or machine learning can both automate and facilitate the ingestion, search, sharing and analysis of digital evidence. For example, it can recognize patterns in digital evidence workflows, and then make suggestions to investigators, including whether a piece of evidence that has not been considered could be useful for the current case. As the quantity of information constantly expands, this kind of proactive prompting in a multi-cloud or on-premise environment will be increasingly important in helping investigators keep on top of the unprecedented quantity of available evidence to improve case resolvability and investigative effectiveness. It can also help facilitate decision-making to resolve recent or active incidents.

A consolidated platform for the continuum of investigation

The growing complexity of a forensics and digital evidence ecosystem requires a tailored, enterprise-integrated approach to help ensure orchestration of the right technologies and workflows across the continuum of a criminal investigation. Dell Technologies solutions help simplify, consolidate, and streamline your organizational deployment process by combining validated workloads and industry-specific software in a scalable, consolidated architecture.

A UNIFIED ENVIRONMENT FOR WORKFLOW MANAGEMENT

Dell Technologies solutions enable the much-needed convergence and integration of different digital forensics and evidence management applications to simplify and automate the workflow. Within the digital evidence management platform, evidence and assets can be annotated and operated upon (e.g., phone and computer data, single-frame extraction from video, audio clips, etc.)—while preserving the original asset and its provenance. Pieces of evidence can also be grouped, linked to each other, and securely shared with stakeholders. AI-driven search features within the platform can further enable investigators to uncover meaningful connections from other cases.

Dell Technologies can also help you federate secure workloads in a cloud environment, an air-gapped on premise environment, or a mix of both. This allows law enforcement professionals the freedom to perform functions including tiering across different levels of retention so that those on the case can work uninterrupted to gain access to and find what they need without requiring additional IT assistance.

TYPICAL USE CASES IN DIGITAL FORENSICS AND EVIDENCE MANAGEMENT

Enabled by Dell Technologies edge, infrastructure, cloud and analytics solutions

SEARCHABLE DATA ANALYTICS

Digital evidence is useful only if the relevant sequences and events can be found. While previously a laborious process performed by law enforcement, now AI can help automate the generation of analysis and tagging. Search capabilities include functions such as displaying a different set of outcomes depending on the user's intentions or searches within controlled vocabularies. The system can find synonyms and use natural language processing to find words with similar sounds. Suggestions can be made as the investigator types. Metadata can also be used in searching, such as GPS locations for where the evidence was recorded or details about who recorded it.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

As well as automating and facilitating ingesting and search, AI can provide further proactive insights. For example, it can recognize patterns in digital evidence workflows and then make suggestions to investigators, including whether a piece of evidence that has not been considered could be useful for the current case, or whether an officer involved is worth talking to for further details. As the quantity of information constantly expands, this kind of proactive prompting will be increasingly important in helping investigators keep on top of the massive quantity of available evidence.

EDITING AND ANNOTATION

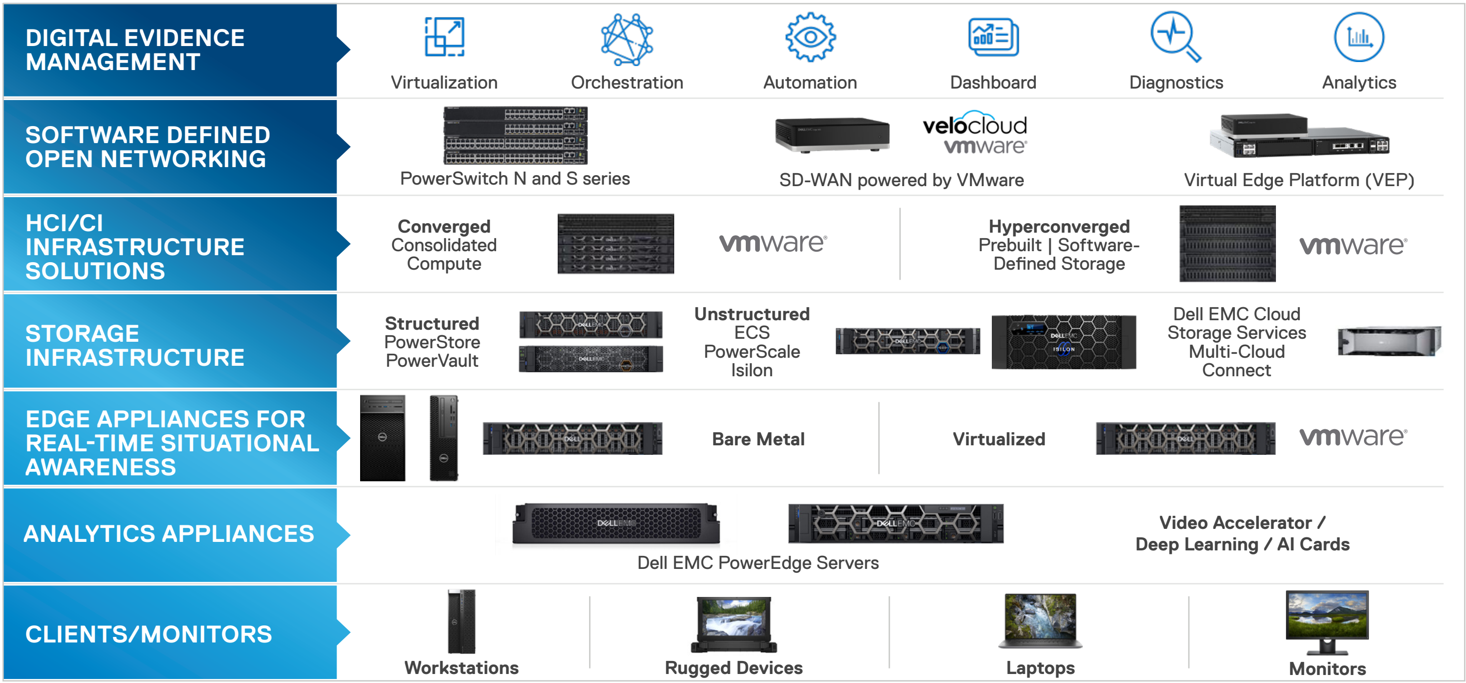
Although the original files must remain inviolable to maintain the chain of custody and keep them admissible as evidence, it is also essential that stages of the investigation can add annotations or operate on them in other ways. For example, a still image or video could be cropped to accentuate a detail, a single frame could be extracted from video showing a crucial event, or faces of incidental bystanders could be blurred out to protect their identities. The original file and details of where it came from must nevertheless still be preserved.

COLLABORATION TOOLS

Criminal investigations by their very nature involve many different stakeholders, from different investigators to alternative agencies to legal teams and judges when cases go to court. Superior officers may be involved, and a case may be transferred between teams. Solid collaboration tools are therefore essential, including the ability to group pieces of evidence and link them or securely share them between stakeholders.

AN INTEGRATED, VALIDATED, AND SECURE PORTFOLIO

Building the foundation for digital forensics and digital evidence management



DIGITAL EVIDENCE MANAGEMENT: Virtualization, Orchestration, Automation, Dashboard, Diagnostics, Analytics

SOFTWARE DEFINED OPEN NETWORKING: PowerSwitch N and S series; SD-WAN powered by VMware; Virtual Edge Platform (VEP)

HCI/CI INFRASTRUCTURE SOLUTIONS: Converged Consolidated Compute; Hyperconverged Prebuilt | Software-Defined Storage

STORAGE INFRASTRUCTURE: Structured PowerStore PowerVault; Unstructured ECS PowerScale Isilon; Dell EMC Cloud Storage Services Multi-Cloud Connect

EDGE APPLIANCES FOR REAL-TIME SITUATIONAL AWARENESS: Bare Metal; Virtualized

ANALYTICS APPLIANCES: Dell EMC PowerEdge Servers; Video Accelerator / Deep Learning / AI Cards

CLIENTS/MONITORS: Workstations, Rugged Devices, Laptops, Monitors

MODERN, SCALABLE IT TO MEET INCREASING WORKLOAD AND DATA DEMANDS

Our expansive range of essential offerings—including servers, storage, software-defined open networking, industry tools for data management, virtualization, and analytics as well as client devices and peripherals—enable law enforcement to do their jobs effectively from aiding with an incident in progress through case resolution.

Dell Technologies provides a tailored solution based on hyperconverged and storage platforms, purpose-built for law enforcement use cases with access to the required system building blocks from distributed locations to a centralized location (on-premise and cloud).

For field operations, our family of compute platforms including networking, ruggedized clients, servers, and edge PCs helps capture, analyze, and gain insights collected from cameras and other sensing devices. For data centers, our range of structured and unstructured storage appliances provides the necessary capacity for the exponential rise of forensics data.

Solutions are purpose-built and designed with the distributed framework needed to easily extend to the data center or cloud, leveraging solutions for downstream investigation, analytics, reporting and archiving on virtualized platforms such as VMware.

Combined with our robust partner ecosystem of systems integrators and solution providers, we help you design, deploy, manage, and scale your digital forensics and evidence management solution as you grow.

AN ON-PREMISE OR MULTI-CLOUD ENVIRONMENT FOR GREATER CHOICE AND ACCESSIBILITY

Dell Technologies provides infrastructure as-a-service offerings to help manage growing IT complexities and scale on demand while controlling costs. With Dell Technologies APEX, IT staff gain access to service management, governance, security, automation, and orchestration tools in a single console for control of IT resources across your on-premise and cloud environments.

AN EXTENSIVE PARTNER PROGRAM TO SUPPORT YOUR SPECIFIC NEEDS

Dell Technologies works with key partners to bring together otherwise fragmented components into a consolidated, streamlined digital forensics and evidence management solution to lower investment risk. Our extensive ecosystem of technology and industry partners helps deliver the tailored approach needed to realize outcomes faster, whether executing simple case workflows or complex, cross-departmental investigations.

INTEGRATED SECURITY TO REDUCE RISK

Dell Technologies helps our customers mitigate cybersecurity risks through our industry-leading hardware and partner offerings. Dell PowerEdge servers, for example, provide hardware-integrated security and resilience to mitigate risks of cyberattacks. The platform delivers features such as trusted remote management, physical intrusion detection, firmware drift detection, seamless automated recovery, easy restore, and the ability to erase sensitive data securely using NIST-approved cryptographic techniques. This ensures that devices and data remain secure and compliant, with strong resilience against cyber threats.

VMware Carbon Black delivers next-generation secure cloud technology to law enforcement agencies while software-defined open networking solutions such as Dell EMC PowerSwitch and SD-WAN powered by VMware help optimize your digital forensics solution. This open-architecture design provides fast and secure access to the needed applications across the entire digital evidence management.

VMware NSX can lock down critical apps, create a logical DMZ in software, and reduce the attack surface of a virtual desktop environment using the segmentation capabilities in NSX. Zero-trust security is now attainable and efficient in private and public cloud environments.

SecureWorks cloud-native solutions for extended detection and response are built on the Taegis Security Operations & Analytics Platform. They leverage its AI-powered analytics and automation engines, curated threat intelligence, and comprehensive attack-vector coverage to help maximize the effectiveness and efficiency of your security program.

A COMPREHENSIVE LAB-VALIDATION TEST APPROACH TO REDUCE TIME TO DEPLOYMENT

To help deliver to your department a digital forensics and evidence management solution that works from day one, Dell Technologies aligns validation standards with our partners to test hardware and software in extreme, real-world scenarios in order to reduce deployment risk. Our global labs enable our customers to have confidence in our solutions and gain access to the latest capabilities on the market while ensuring optimization of workflow-specific applications through access to developer support resources.

A TRUSTED PARTNER TO MOVE YOUR ORGANIZATION FORWARD

At Dell Technologies, we understand that you require a fully-integrated, secure digital forensics and evidence management solution designed to help turn your data into information-driven outcomes.

Our end-to-end approach to data management using a centralized, multi-use platform helps deliver results at every stage of the investigation to maintain searchable, compliant historical archives.

Our comprehensive solutions portfolio and data management expertise help reduce the risk, cost, and complexity of implementation by leveraging the right mix of technologies to fit your specific use case requirements. In addition, our advisory, design, build, integration, and lab validation services help deliver an edge-to-core-to-cloud digital forensics and evidence management system that streamlines deployment with orchestration and automation.

Dell Technologies has been serving law enforcement agencies with a global team of dedicated subject matter experts for many years. As the criminal investigation landscape evolves, Dell Technologies is committed to continued innovation in digital forensics and evidence management with significant investments allocated towards research and development of next generation forensics and computer vision technologies. This commitment extends to providing you with an open and scalable infrastructure designed to deliver results from day one and as needs change—helping you to transform your department with data-driven insights that empower and protect the public you serve while equipping forensic investigators and officers with the right data and tools at the right time to do their jobs with efficiency, safety, and accuracy.

Learn more about our Safety and Security | Computer Vision solutions.

Contact a Safety and Security | Computer Vision expert.

Connect with us.

[1] 2021 Video Evidence Trends Report sponsored by iNPUT-ACE.