Cellebrite

2025 Industry Trends Survey

Transforming Digital Investigations in public safety

Introduction

In our modern world – nearly everyone carries with them a digital witness – from mobile phones to wearable technology that tracks movements, lifestyles and habits – helping to map out where we go, who we are and with whom we interact.
When crimes happen, this digital data becomes essential to finding the truth.

Cellebrite's 2025 Industry Trends Survey, now in its sixth year, offers a comprehensive look into the transformation of digital forensics and its profound impact on modern investigations.

As digital footprints become increasingly central to criminal activities and subsequent investigations, this thorough analysis reveals how law enforcement agencies are adapting their methodologies and embracing new technologies.

The data reveals a growing traction for cloud-based solutions, a significant shift in the role of digital evidence in solving cases, and for the first time, we're getting insights into Artificial Intelligence adoption.

Some key findings include:

98%

Nearly all prosecutors report that digital evidence is pivotal in successful prosecutions, with more than half stating it is more crucial than DNA in modern cases.

61%

of respondents view artificial intelligence (AI) positively, recognizing its potential to enhance efficiency, accuracy and speed in investigations.

80%

Approximately 80% of respondents believe AI-powered solutions simplify investigative processes by automating tasks and identifying critical evidence faster.

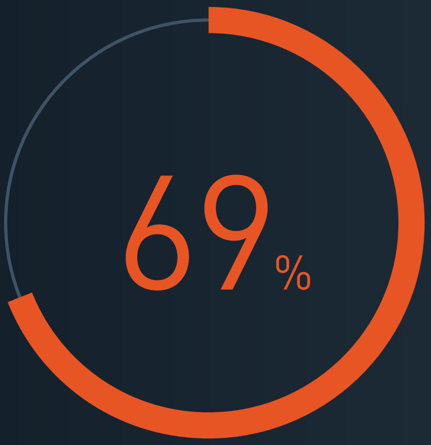
40%

Despite some hesitancy, nearly 40% of agencies are open to using cloud technologies for evidence storage and sharing, citing its scalability and security advantages.

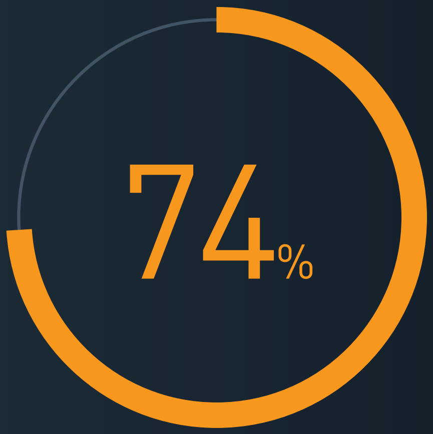
Investigators are also navigating how to manage the ever-increasing volume of digital data. On average, each case now has between two and five devices which must be analyzed, leading to an overwhelming amount of evidence and case backlogs.

In this whitepaper, we break down challenges agencies face today including the explosive growth of data and digital devices, clearing backlogs, locked devices and encrypted apps.

We will focus specifically on how each role within an agency isimpacted by these obstacles and how advanced forensics solutions can help.



stated that the investigative team does not have enough time to review all the data.



of investigators search publicly available information online about a person of interest daily or multiple times a day.

How AI Transforms Digital Forensics and Investigations

For the first time, this year's survey is giving us a deeper understanding of how AI is revolutionizing digital investigations by addressing the exponential growth of digital evidence. While agencies show increasing enthusiasm, there's a nuanced understanding of both AI's potential and its regulatory challenges.

Perception and Adoption of AI

The digital forensics community is experiencing a significant technological shift with artificial intelligence in the mix.

Three in 10 respondents encountered more AI-related crimes and at the same time, 64% believe AI can help reduce crime, with approximately 80% of respondents viewing AI as a tool that makes investigations easier, contributing to faster and more effective results.

This significant majority underscores the increasing recognition of AI's practical benefits, particularly its role in speeding up investigative processes. More than half of the agencies (**51%**) are strategically planning AI technology integration within the next two years, signaling a proactive approach to technological advancement.

Despite widespread optimism, a cautious undercurrent exists. While **79%** acknowledge AI's investigative improvements, **60%** express concerns about potential regulatory constraints that might limit its full implementation.

51%

strategically planning AI technology integration

79%

acknowledge AI's investigative improvements

60%

express concerns about potential regulatory constraints

Impacts on Investigations

The current investigative landscape is characterized by data overwhelm. Examiners consistently report **3 to 4 weeks** of digital forensic examination backlogs, highlighting the critical need for innovative solutions. Investigators are particularly stretched, with **69%** struggling to comprehensively review case data.

90% of respondents say AI can positively impact digital investigations, especially with its ability to analyze vast datasets, recognize patterns and detect anomalies.

3 - 4 WEEKS

of digital forensic examination backlogs

64%

believe AI will help reduce crimes

86%

agree AI can accelerate large-volume data analysis

82%

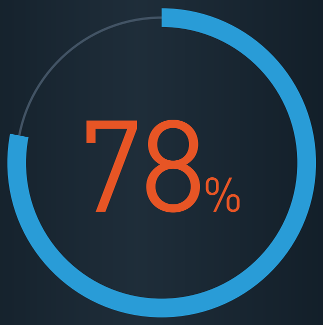
say Ai can automate repetitive tasks like keyword searches and report generation

60%

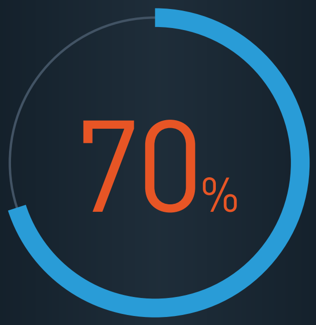
agree that AI reduces human error and prioritizes evidence

Most Valued AI Functionalities

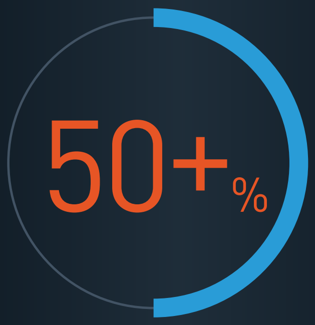
Survey participants identified the most impactful AI features:



prioritize content classification and evidence prioritization



value automated device extraction and lead identification



appreciate tools for generating investigative reports and automating forms

AI and Cloud Integration

The collaboration between AI and cloud technologies has created a powerful ecosystem for digital forensics, establishing new standards for evidence processing and analysis. This combination addresses multiple critical challenges that have historically hindered digital investigations.

By combining the processing power of AI with the scalability of the cloud, agencies are now able to tackle some of the most pressing challenges in modern investigations—specifically the need for rapid data analysis and secure, efficient storage.

Cloud-based solutions provide investigative teams with the ability to store and access vast amounts of digital evidence in real-time, without being constrained by the physical limitations of traditional on-premise storage.

Coupled with AI's ability to rapidly analyze this data, agencies can now automate many aspects of the investigative process. From evidence categorization to pattern recognition, these technologies reduce manual workloads and ensure critical information is identified and prioritized more effectively.

Digital Forensic Units (DFUs)

The Diversification of Digital Evidence

Examiners

Digital forensic examiners increasingly face a wide array of devices, reflecting the rapid technological diversification in criminal investigations. While 94% of examiners report frequently encountering smartphones, other device types are also on the rise:

Drones
225% INCREASE

Cryptocurrency
187.5% INCREASE

Wearables
125% INCREASE

Vehicles
91% INCREASE

On average, examiners handle **2 to 5 devices per case**, signaling a pressing need for advanced forensics tools to manage the surge in digital evidence complexity.

2 to 5
DEVICES PER CASE

Getting the Most Data

Despite expectations, accessing 100% of a device's data is rarely possible. Cellebrite's survey shows **75% of extractions leverage Full File System (FFS)** or physical extractions, but achieving these results requires the latest technology.

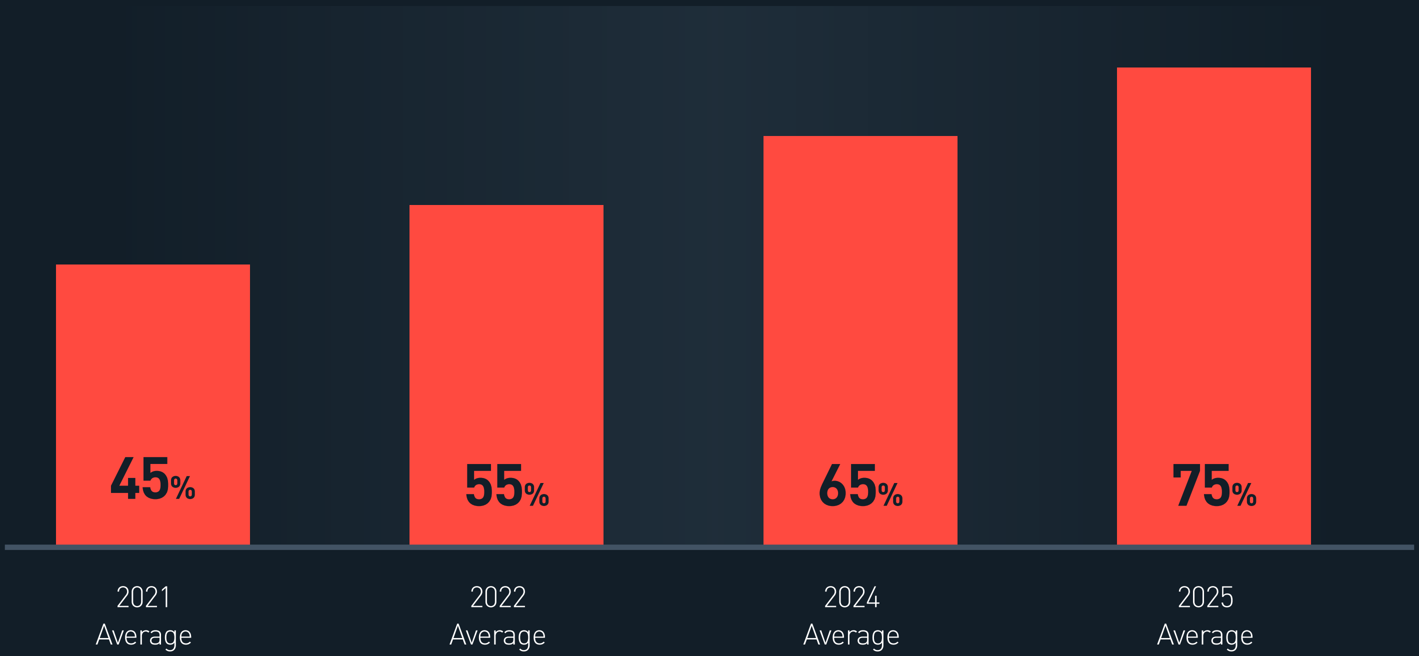
Full File-System Extraction Vs. Logical Extraction

Digital forensics experts gather evidence from smartphones, wearables, personal computers and digital media using different methods. Two key techniques are Full File Sytem Extraction and Logical Extraction, each with its own advantages and limitations tailored to the specific case.

	Full File Sytem Extraction (FFS)	Logical Extraction
Definition	Extracts all accessible data, including deleted files and file structure without needing an Application Programming Interface (API)	Extracts only active, logical data from the device via an Application Programming Interface (API)
Data Access Level	Accesses visible and hidden system files, full database files, app data, metadata and can often decrypt encrypted files.	Limited to user-level data, that is visible to the operating system (OS), i.e., contacts, messages, call logs.
Deleted Data Recovery	Can retrieve deleted files and fragments, if not overwritten.	Cannot recover deleted data.
Extraction Speed	Slower due to larger data volume and more complex data layers.	Generally faster due to smaller, active data selection.
Setup and Requirements	More device-dependent, may require specialized tools or root access.	Works on a wider range of devices with minimal setup.
Application Scenarios	Suitable for in-depth forensic analysis where complete data is needed.	Ideal for quick investigations where only active data is relevant.

Criminals are increasingly using encrypted apps, like Telegram, to conduct their activity. Decoding this data is a significant challenge for agencies relying on outdated forensic solutions.

In The Past Three Months, Of All The Mobile Extractions You Performed, What Percentage Were Physical / Full File System Extractions?



Key Challenges Faced by Examiners:

Locked Devices:

A significant challenge for examiners is dealing with locked devices. Approximately two-thirds of the devices they encounter are locked, hindering access to crucial digital evidence.

Encrypted Apps

The prevalence of encrypted apps further complicates digital examinations as these apps create barriers to data extraction and analysis.

Extraction Time

The time-consuming nature of extraction processes remains a persistent challenge, impacting case turnaround times.

Key Insight: Year-over-year, these challenges are growing, and examiners are feeling the pressure. **40% report the majority of their workload involves data analysis to generate leads** and solutions to expedite this time-consuming process are urgently needed**.**

Workload and Training

Although there has been a slight increase, **only 48% of examiners** have advanced or extensive formal training — a modest improvement from the **previous year's 39%**. This highlights a pressing need for cutting-edge solutions and resources to keep pace with these trends.

Agencies that do not adopt advanced digital evidence solutions risk being left behind as cybercriminals evolve their methods.

Investigative Units

Investigators

Investigative units are at the forefront of digital investigations but are constrained by the vast amounts of data they must manage. According to our survey, **68% of investigators** report time constraints that prevent thorough data analysis.

40%

report the majority of their workload involves data analysis

48%

have advanced or extensive formal training

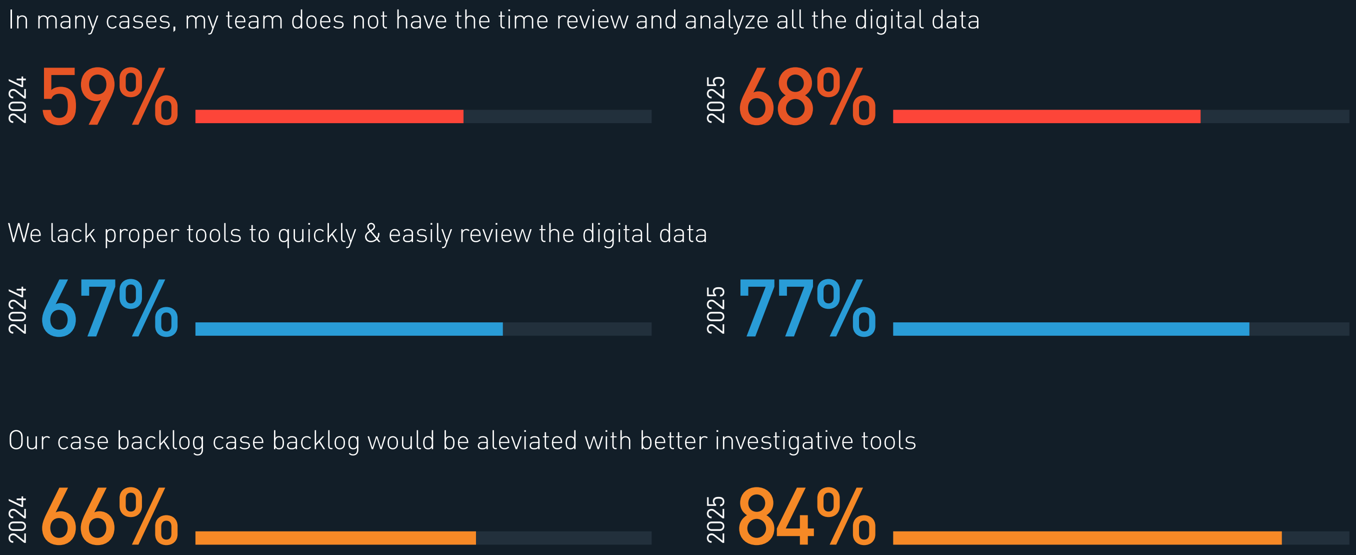
68%

report time constraints that prevent thorough data analysis

This issue is exacerbated by the volume of digital content involved. Investigators are reviewing **2 to 5 devices per case,** equating to an average of **69 hours per case.** This increasing workload highlights the need for optimized workflows to keep pace with growing demands.

2-5
DEVICES
per case
=
69
HOURS
per case

To what extent do you agree/disagree with the following statements:



Key insight: To meet these challenges, investigators must focus on enhancing efficiency, streamlining workflows and enabling comprehensive data review to ensure that critical evidence is not overlooked.

Investigators are increasingly turning to online research for leads.

71% of investigators conduct daily online searches, yet the manual nature of these searches can be time-consuming and inefficient. There's a clear need for more scalable and efficient tools to automate data collection and filtering, allowing investigators to focus on higher-value tasks.

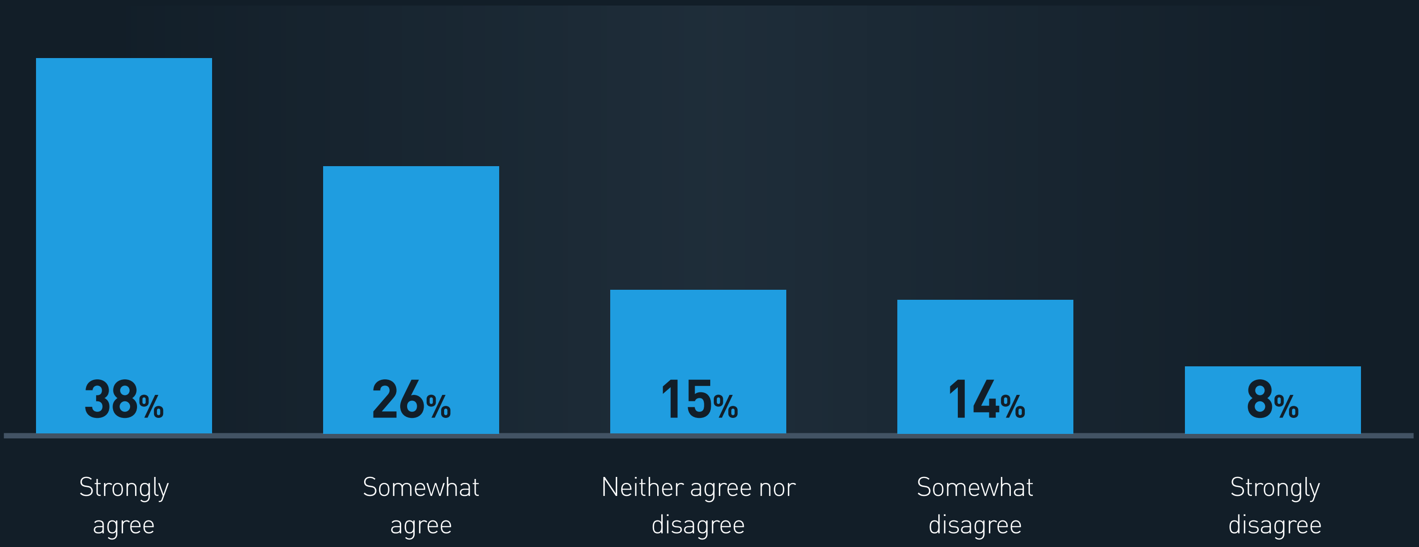
Key insight: AI-powered solutions help increase efficiency in going through the data to find relevant details and uncovering hidden connections. About 9 in 10 noted AI can positively impact investigations with improved pattern recognition and faster analysis of large data sets.

Analysts

Analysts, on the other hand, dedicate substantial time to digital evidence review. More than half **(51%) regularly conduct online searches. On average,** analysts spend **61 hours per case** analyzing data from devices. This intensive process involves reviewing photos, videos and text messages, often requiring cross-referencing multiple datasets to identify patterns.

61
HOURS PER CASE

To what extent do you agree/disagree with the following statement: The first thing I do at the beginning of the case is search online for information about a person of interest (social media, public database)



Key Insight: AI-powered solutions like Pathfinder have proven to be game changers for analysts. Survey findings reveal that Pathfinder can reduce case processing times by **50%**, allowing analysts to focus on critical decision-making tasks. This emphasizes the need for greater use of AI analytics to achieve faster insights and better pattern recognition.

Agency Management

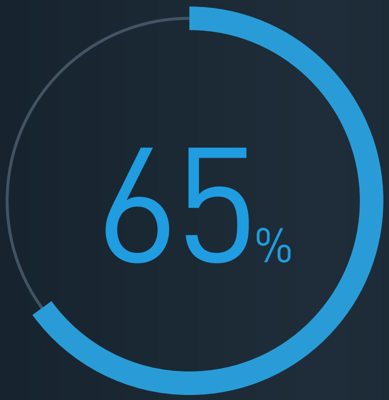
Agency Managers & Command Staff

Agency management sees digital evidence as key to community safety, with **65%** attributing high importance to digital investigations.

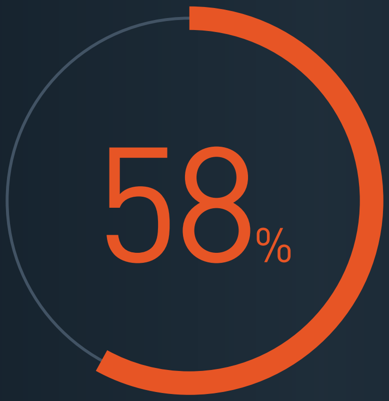
58% say they need to improve their current data management practices. In our modern world, smartphone technology and social media use is prevalent and leaves behind a detectable digital footprint. Criminal activity is no exception, and technology plays a huge role in investigating modern crimes.

The key question is whether evidence management practices are keeping up with the rising rate, volume and variety of data of today—and more importantly, of tomorrow.

New methods of finding and presenting evidence in court may turn up in the near future and agencies need to ensure they are fully equipped to manage every detail of an investigation, no matter how peculiar.



attributing high importance to digital investigations



need to improve data management practices

Key Insight: Comprehensive, end-to-end solutions are essential, addressing the lifecycle of digital evidence from extraction and analysis to secure sharing, supporting effective decision-making and resource allocation.Involving many functions and departments, investigations run more smoothly when the right tools are used to address workflow challenges and inefficiencies.

With decision-making inextricably linked to evidence sharing, law enforcement professionals are beginning to emphasize the importance of accessible case information around the clock, up-to-date and error-free.

The uptick in sentiment toward digital evidence and improving data management practices can also be attributed to the fact that agency managers collaborate cross-jurisdictionally to tackle complex and larger cases. The days of traveling between stations to deliver physical evidence are phasing out as investigators need to outpace an always evolving world. Reducing time-to-closure with faster collaborations is paramount to staying ahead of criminals, who use the latest technology to perpetrate crimes.

Challenges and Needs:

Funding Constraints:

65%

of agency management stated that the lack of further investment in digital investigative solutions will have a moderate or significant impact on their ability to effectively investigate cases.

Data Growth:

On average, agency management has noted a

76%

growth in digital data from devices over the past 3 years.

These observations align with the often-quoted Moore's Law—which projects that the number of transistors on a computer chip to double every year.

Along with this exponential increase came the boom in digital storage space and consumer data. About 10 years ago, 1 TB of solid-state (SSD) data cost roughly $1,000. Today, that same capacity costs just under $100*.

Consequently, video and image file sizes have grown as smartphones continue to offer higher resolution cameras and processing power increases. This upscale in data fidelity gives digital forensics examiners ample opportunity to extract meaningful information.

And yet, the growing size of these files is a double-edged sword—requiring more computing power and specially designed forensic tools to analyze.

About 10 years ago, 1 TB of solid-state (SSD) data cost roughly

$1,000

Today, that same capacity costs just under

$100

*https://ourworldindata.org/data-insights/the-price-of-computer-storage-has-fallen-exponentially-since-the-1950s

Cloud & Sharing Data

Barriers and Bottlenecks in Current Digital Evidence Sharing Practices

Despite the growing interest in cloud-based solutions, many law enforcement agencies continue to struggle with traditional methods for sharing and managing digital forensic data. The frustrations around these outdated practices are numerous:

Cumbersome and Slow Data Transfer

Many investigators report that transferring data via USB connections can be slow and inefficient, leading to significant delays in the investigation process.

Difficulty Accessing External Hard Drives

Access to external hard drives can be cumbersome, with issues related to compatibility, speed and data retrieval, further hampering the efficiency of data sharing. further hampering the efficiency of data sharing.

Lack of Cloud Access

Without access to cloud storage, many agencies are still forced to rely on physical media, which creates further logistical challenges in storing and sharing large volumes of data securely.

Security and Chain of Custody Issues

Relying on hard media such as USB drives and external hard drives presents ongoing challenges related to chain of custody, data loss, security breaches and the risk of theft or damage. These issues not only complicate investigations but also undermine the integrity of digital evidence.

Increased Travel and Expenses

The need to physically transfer data or collect exhibits from multiple locations increases travel time and associated costs. Sourcing external drives and other necessary equipment is also expensive, adding to the financial burden on agencies.

Data Loss and Corruption

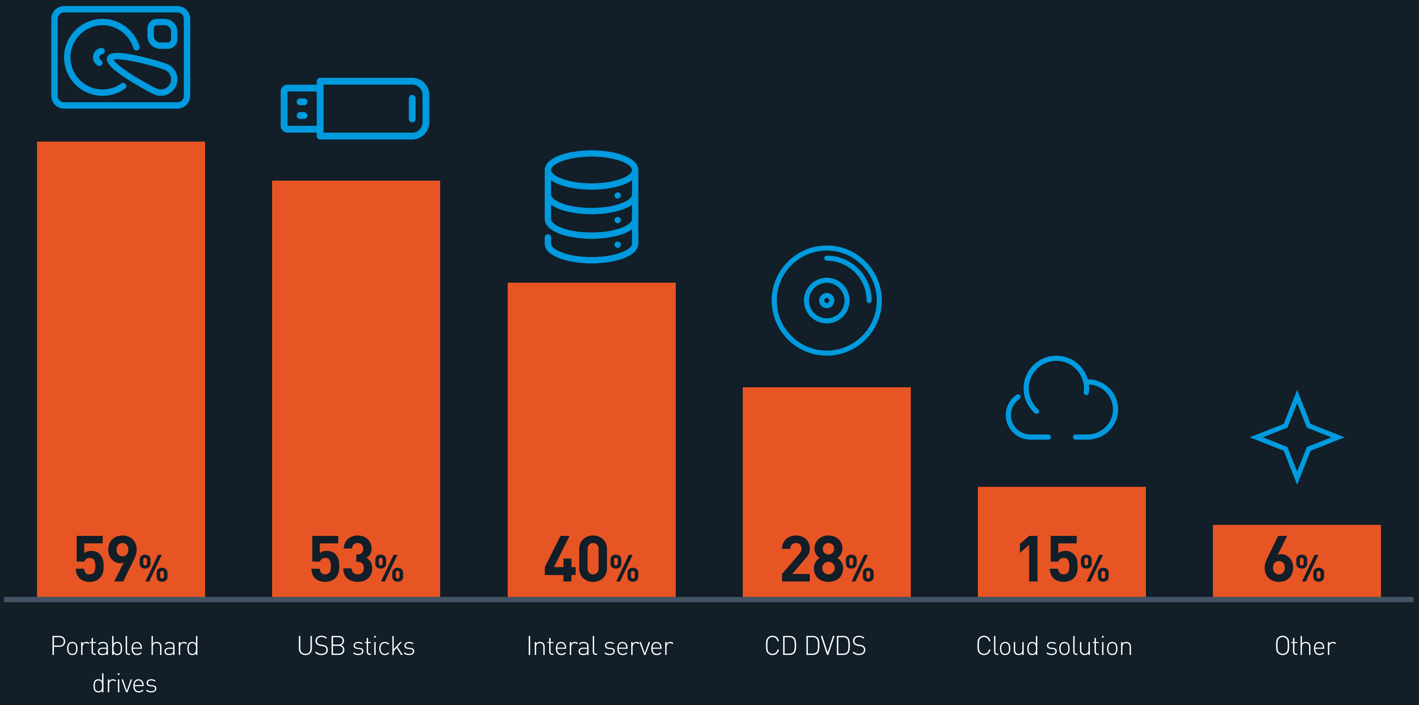
The risk of data loss, theft or corruption remains a significant concern with traditional storage methods, as these media can be damaged or misplaced, compromising the investigation.

These frustrations highlight the broader need for more modern, secure and efficient solutions that can address the ongoing limitations of current practices.

Evidence Management and Storage

While many agencies still rely on traditional internal servers, homegrown systems or even USB sticks for storing critical digital evidence, the growing volume and complexity of data is creating a pressing need for more advanced solutions. The cloud has emerged as a compelling alternative, offering the scalability, security and efficiency needed to manage the burgeoning digital evidence load.

How do you share digital forensic data and reports within your agency?



Cloud Adoption and Management

Despite the growing interest in cloud storage, the adoption rate remains gradual. Approximately **38% of agency management** and **40% of investigators** are open to using cloud storage for digital evidence; however, concerns around cost, data security and legal compliance continue to act as significant barriers. These concerns highlight the complex nature of transitioning from traditional storage methods to more modern cloud solutions.

40%

of investigators are open to using cloud storage for digital evidence

Key Insight:

While challenges remain, there is a noticeable trend toward cloud adoption, as agencies are increasingly recognizing its value for securely storing and accessing evidence. The ability to quickly scale storage as data volumes grow is particularly appealing, as is the potential to streamline evidence sharing and access across various departments and jurisdictions.

Challenges and Needs:

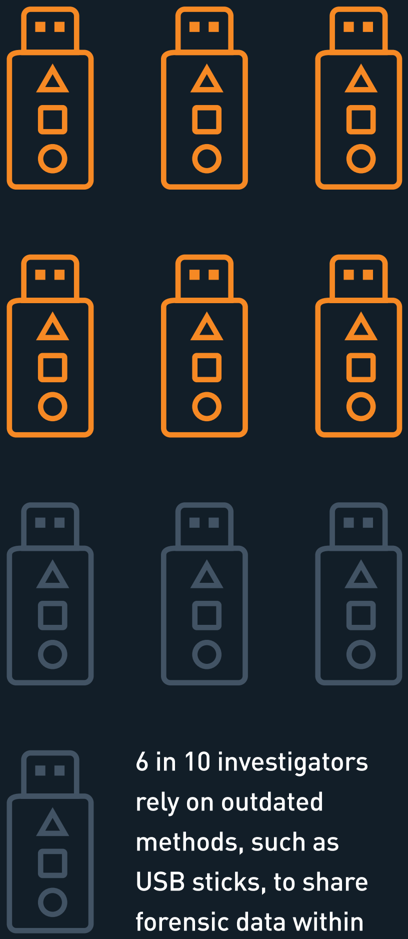
Two major challenges are currently affecting how digital evidence is shared and reviewed:

Data Sharing:

6 in 10 investigators rely on outdated methods, such as USB sticks, to share forensic data within their agencies. This reliance on physical storage devices underscores the need for more efficient and secure data-sharing methods, especially as digital evidence grows in size and sensitivity.

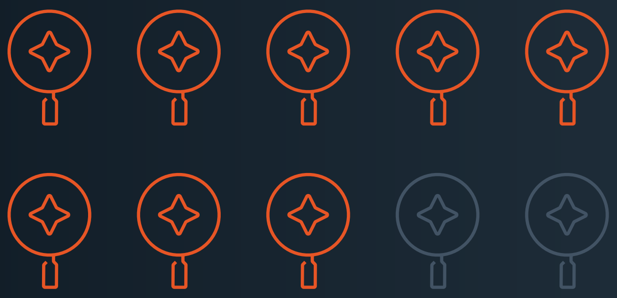
However, there is a better way. Agencies that adopt cloud-based solutions can alleviate these pains. Moreover, cloud-based solutions can provide better collaboration between the digital forensic lab and the investigative team.

With cloud-based solutions, examiners can share their preliminary findings with investigators accessible with just an internet browser, and investigators can better focus their ongoing investigations based on data they are seeing from devices. This is especially helpful since the survey found challenges in data review.

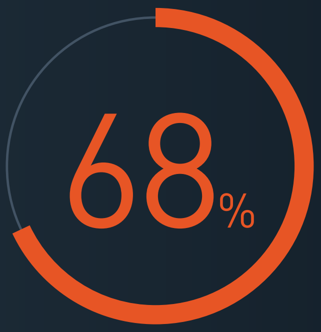


6 in 10 investigators rely on outdated methods, such as USB sticks, to share forensic data within their agencies.

Data Review:

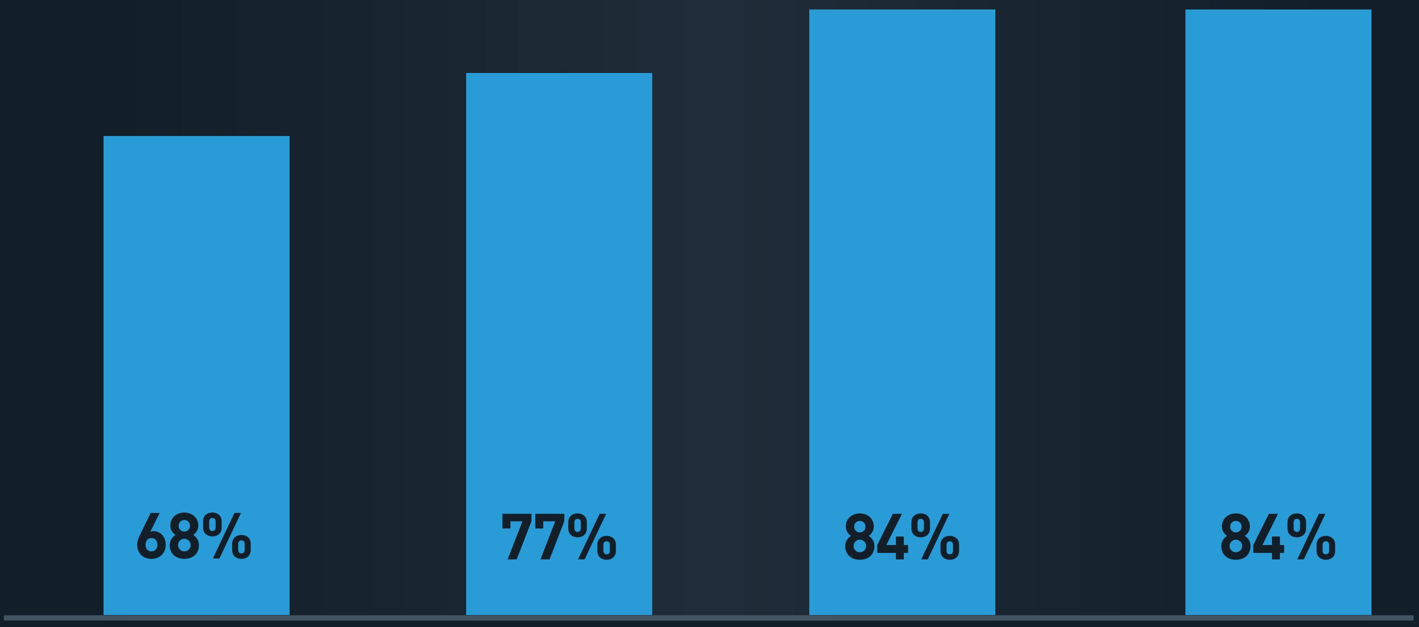


8 in 10 investigators report lacking the necessary tools to easily review digital data, hindering their ability to efficiently analyze evidence.



of investigators admit they do not have enough time to fully review all the data available to them, which can lead to delays in case resolution.

To what extent do you agree/disagree with the following statements:



In many cases, my team does not have the lime to review and analyz all the digital data

We lack proper tools to quickly & easily review the digital data

Our case backlog would be alleviated with beller investigative tools

AI can speed up investigations

✦ NEW ✦

Prosecutors are also increasingly recognizing the crucial role of digital evidence in securing successful prosecutions. According to recent surveys, **98% of prosecutors** agree that digital evidence is essential to their cases, and **81%** feel confident in presenting this evidence in court.

Key Insight: There is a clear need for secure, interoperable solutions that make the sharing of digital evidence between law enforcement and prosecutors faster and easier.

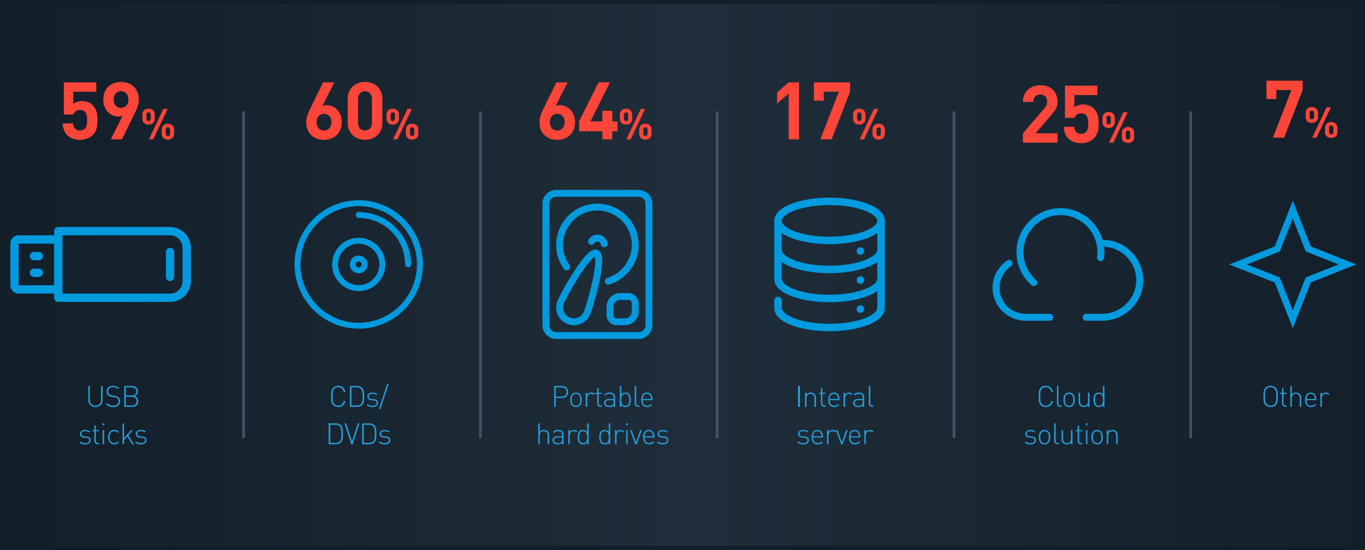
This would help alleviate the frustrations many face with current data-sharing methods, ensuring more efficient and effective collaboration.

Challenges and Needs:

Data Sharing Methods: Despite advancements in digital tools, portable hard drives, DVDs and USB sticks remain the primary methods used by prosecutors to collaborate with law enforcement when sharing forensic data.

Frustration with Data Sharing: Approximately one-third of prosecutors report feeling extremely or significantly frustrated with the current practices for sharing digital forensic data. This frustration is largely due to slow transfer speeds, security concerns and the logistical challenges of managing physical media.

How do you collaborate and share digital forensic data and reports with law enforcement?



Conclusion

The demands of modern digital investigations call for integrated, scalable solutions. From data extraction to secure sharing and courtroom presentation, agencies require end-to-end solutions for more efficient and effective operations which seamlessly manage the entire digital evidence lifecycle.

Cellebrite's suite of AI-powered and cloud-enabled solutions provides agencies with scalable, secure platforms that automate workflows, reduce manual effort and ensure the integrity of digital evidence across every stage of an investigation.

Leveraging these solutions will enable agencies to create faster and simpler workflows and automate repetitive tasks and evidence prioritization—common investigation bottlenecks. Ultimately, agencies can reduce case backlogs and accelerate case resolutions. This allows investigators to focus on high-priority tasks, overcoming resource constraints.

Adopting scalable, integrated solutions like those offered by Cellebrite empower agencies to efficiently manage the increasing volumes of digital evidence.

They enhance operational collaboration and security in investigations, aligning digital forensics processes with today's public safety goals. In this rapidly evolving digital landscape, comprehensive solutions are no longer optional but essential to ensure justice is served.

Explore More on the 2025 Industry Trends Survey

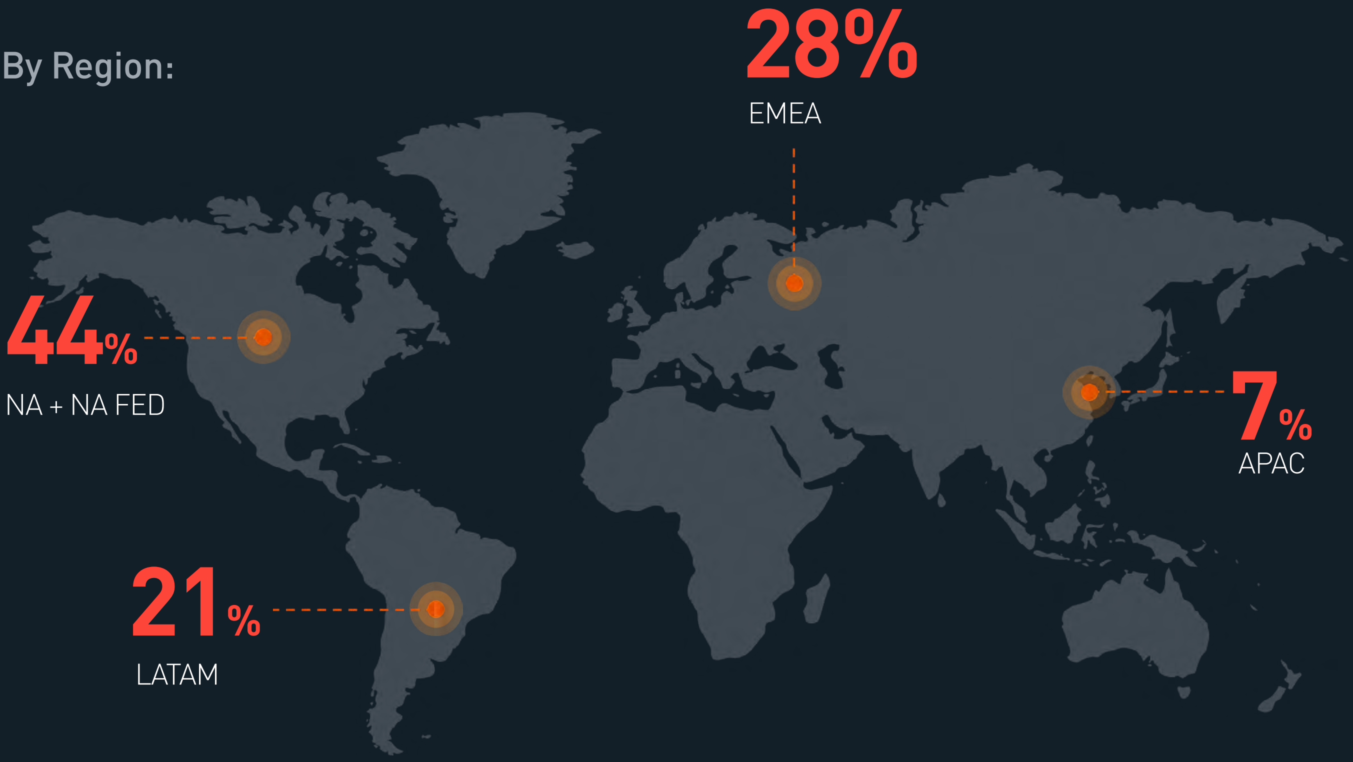
To access valuable content on the future of digital forensics and law enforcement investigations, visit our dedicated page with additional resources.

Scan the QR code to stay updated with the latest trends, insights and advanced solutions driving the transformation of digital investigations.

Methodology

With more than 2,100 responses from law enforcement professionals in nearly in 100 countries, including forensics examiners, investigators, analysts, prosecutors and agency managers, the 2025 survey uncovers the challenges agencies are facing with digital evidence.

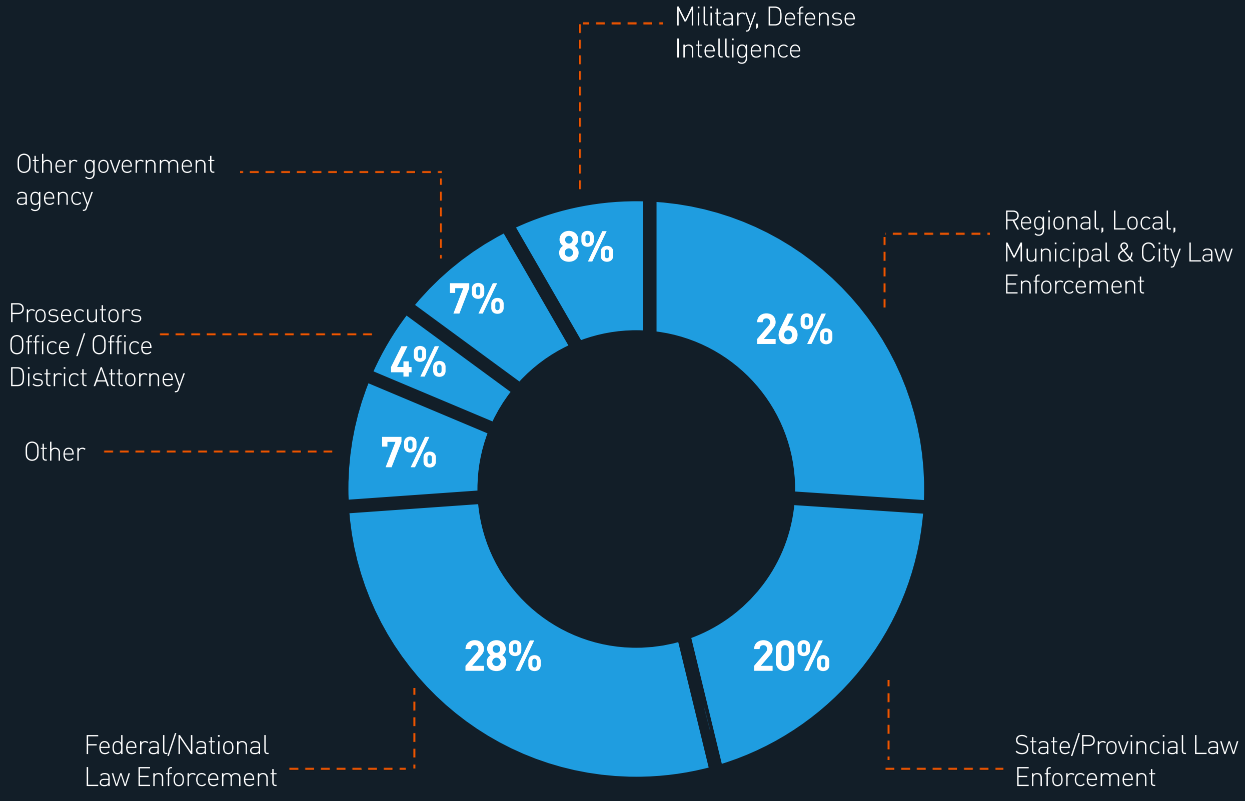
By Region:



Respondents from the survey represent a range of agency types and sizes globally, including federal or national agencies, military and intelligence organizations, state, city and local law enforcement agencies including large cities, small departments and sheriff's offices.

The online survey was conducted during Q3 2024, and was promoted online through email, industry forums, listservs, social media and third-party media outlets. The data was subsequently reviewed and cleansed to ensure the highest accuracy. The data was then analyzed to present the findings within this whitepaper.

By Agency Type:



Cellebrite | Justice Accelerated

About Cellebrite

Cellebrite's (Nasdaq: CLBT) mission is to enable its customers to protect and save lives, accelerate justice, and preserve privacy in communities around the world. We are a global leader in Digital Investigative solutions for the public and private sectors, empowering organizations in mastering the complexities of legally sanctioned digital investigations by streamlining intelligence processes. Trusted by thousands of leading agencies and companies worldwide, Cellebrite's AI-powered Case-to-Closure platform transform how customers collect, review, analyze and manage data in legally sanctioned investigations.

- To learn more visit us at www.cellebrite.com
- Contact Cellebrite globally at www.cellebrite.com/contact