MAGNET FORENSICS®

carahsoft.

Practical Solutions for Digital Forensics Challenges in the Public Sector

Thank you for downloading this Magnet Forensics resource. Carahsoft is the distributor for Magnet Forensics Law Enforcement solutions available via NASA SEWP V, ITES-SW2, and other contract vehicles.

To learn how to take the next step toward acquiring Magnet Forensics' solutions, please check out the following resources and information:

For additional resources:
carah.io/MagnetForensicsResources

For additional Magnet Forensics solutions:
carah.io/MagnetForensicsSolutions

To set up a meeting:
MagnetForensics@carahsoft.com
571-662-3150

For additional Law Enforcement solutions:
carah.io/LawEnforcement

To purchase, check out the contract vehicles available for procurement:
carah.io/MagnetForensicsContracts

For more information, contact Carahsoft or our reseller partners:
MagnetForensics@carahsoft.com | 571-662-3150

MAGNET FORENSICS®

Navigating digital investigations:

Practical solutions for digital forensics challenges in the public sector

A guide for U.S. federal civilian digital forensics teams and their leaders on conducting investigations, examining mobile devices, and leveraging automation

Contents

Introduction

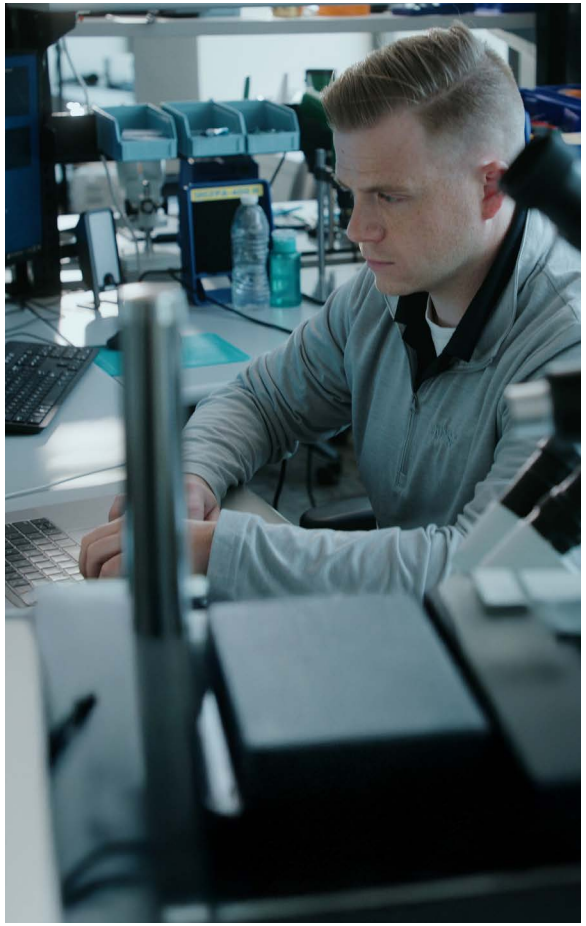
Federal civilian agencies—including the Securities and Exchange Commission (SEC), the Office of the Inspector General (OIG), the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the U.S. Secret Service—are at the forefront of investigating complex criminal activities such as financial fraud, cybercrimes, corruption, human trafficking, and organized crime.

Digital forensics has evolved into a critical aspect of these investigations.

However, the increasing volume and complexity of digital evidence present significant challenges. Once managed by investigators with basic technical skills, the field now requires specialized expertise that agencies struggle to recruit and train quickly enough. This gap has led to mounting case backlogs and inefficiencies, exacerbated by the reliance on disparate tools that hinder workflows.

A global leader in providing digital investigative solutions, Magnet Forensics can help you capture, examine, report on, and manage evidence from a wide range of digital sources, including mobile devices, computers, IoT devices, and cloud services. A trusted partner worldwide, Magnet Forensics' solutions are used by more than 4,000 public and private sector organizations across over 90 countries.

This guide is divided into three sections, each focusing on the challenges faced by digital forensic laboratories in contemporary investigations. In each section, we will explore common issues and provide practical solutions to help meet the investigative needs of your agency both now and in the future.



Tackling modern digital investigations

Digital investigations require advanced tools and expertise to navigate the complexities of evolving technology.

Investigators must analyze vast amounts of digital evidence from various sources, including computers, mobile devices, and cloud platforms, while ensuring data integrity and compliance with legal standards.

As digital threats against federal agencies continue to rise, forensic professionals must stay ahead with innovative technologies that enhance efficiency and accuracy in uncovering critical evidence.

The challenges of digital forensics

Digital forensics has long been essential in investigating financial fraud, corruption, human trafficking, organized crime, cyber-enabled offenses, and other cases involving digital evidence. As digital threats continue to evolve, federal civilian agencies face growing challenges in conducting those investigations. The rapid advancement of technology—combined with increasingly sophisticated cyberattacks—has made the task of investigating and recovering digital evidence more complex than ever. This complexity continues to grow due to several key factors:

Encryption and security measures:

With the rise of encryption technologies and sophisticated security protocols, gaining access to critical evidence has become a significant hurdle. Most modern devices employ advanced encryption methods, making it difficult for investigators to access and analyze stored data.

Volume and diversity of data:

Federal agencies must sift through vast amounts of data stored across multiple devices, platforms, and cloud environments from computers, mobile devices, cloud storage, and IoT devices. Agencies are under constant pressure to identify, contain, and recover from cybersecurity incidents, yet the sheer volume and variety of data make it challenging to extract, analyze, and correlate evidence efficiently.

Evolving technologies:

As technology continues to advance, so do the methods and tools used by criminals. Federal agencies must stay ahead of new operating systems, emerging devices, and evolving security features that can impact the collection and analysis of digital evidence in investigations.

Collaboration barriers:

Siloed data and fragmented collaboration get in the way of the efficiency and effectiveness of digital investigations. Integrated platforms and interoperable systems are needed for seamless information sharing and collaboration across departments and agencies. Breaking down silos enhances investigative outcomes by facilitating comprehensive data analysis and collaborative decision-making. Expedited case processing (and innovative strategies to get there) is extremely valuable to help examiners get ahead of cases that are always waiting in the wings.

Digital investigations in the mobile era

With the widespread use of smartphones, cloud services, and encrypted apps, investigators struggle to collect, analyze, and interpret evidence from mobile devices.

These devices store vast amounts of data, including messages, photos, videos, location data, and app histories, which are essential for investigations.

However, encryption and evolving security methods make it difficult for investigators to access this information.

The rise of mobile technology requires specialized tools to address these challenges.

Mobility is reshaping digital forensics

Mobile devices are now at the center of digital investigations, creating both opportunities and obstacles for federal agencies. The widespread use of smartphones, tablets, and other portable devices has changed both how criminals operate and how evidence is collected. Several key challenges arise from this shift:

Encrypted and locked devices:

Modern mobile devices employ robust security measures—including encryption and biometric authentication—to protect user data. This makes it difficult for investigators to gain access to crucial evidence.

Wide variety of devices, operating systems, and applications:

The rapidly evolving mobile security landscape—with new device models and operating systems being released and updated regularly—presents an ongoing challenge for investigators. Keeping pace with these changes and ensuring forensic tools are compatible with a wide range of devices is essential, but often difficult.

Cloud storage and data synchronization:

As mobile devices increasingly sync data to the cloud, investigators must contend with the challenge of accessing information stored off-device. This can make it harder to locate and extract the full scope of relevant evidence, as cloud storage providers may have different protocols for handling and sharing data.

Volume of data:

Mobile devices store an immense amount of personal and sensitive information, including call logs, text messages, location data, photos, and app histories. The sheer amount of data complicates investigations, requiring specialized tools to process and analyze the information efficiently.

Reshaping the war against terrorism, extremism, and drug cartels

In counterterrorism cases, the speed of data analysis is crucial. The ability to quickly process, analyze, and act on digital evidence can mean the difference between stopping an attack and missing a window of opportunity. Magnet Forensics provides agencies with the necessary tools to handle the volume and complexity of modern digital investigations.

Advanced media analysis for modern threats

Magnet Forensics is transforming the landscape of criminal investigations, enabling law enforcement and intelligence agencies to combat terrorism, violent extremism, and organized crime with unprecedented speed and precision. By combining AI-driven media classification, facial recognition, and natural language processing, our tools accelerate the analysis of massive volumes of digital content—including images and video—while reducing the manual burden on investigators.

Media classification tools such as Magnet Griffeye help law enforcement and forensic analysts identify and prioritize potentially relevant or illegal material. By automatically detecting categories like child sexual abuse material (CSAM), weapons, narcotics, or extremist imagery, classification tools can accelerate case workflows, surface critical evidence sooner, and reduce the need for investigators to manually review every file. This not only saves time but also reduces the emotional toll associated with viewing disturbing content. Ultimately, media classification enables more focused and efficient investigations.

Improving efficiency with automation

Automation is a game-changer in digital forensics, offering substantial time savings and enhancing the accuracy of investigations.

Automated workflows reduce the manual workload, allowing forensic investigators to give their time and expertise to more complex and critical aspects of an investigation.

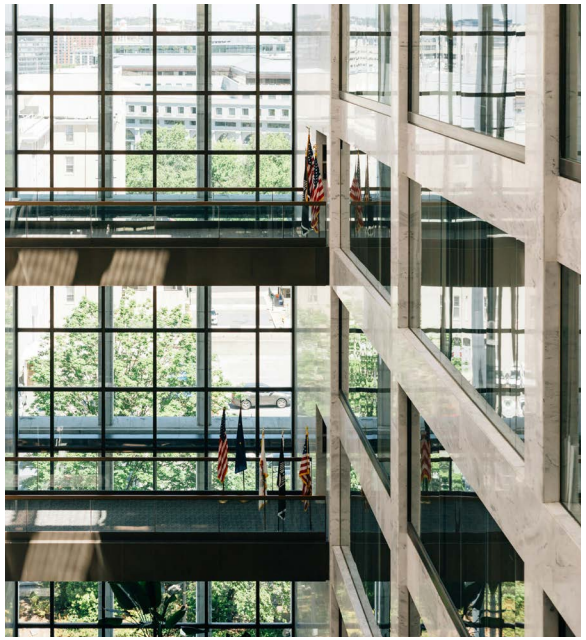
Automation can enable investigators to focus on uncovering deeper insights that might otherwise be missed.

Managing growing data volumes with limited resources

The volume of data that federal agencies must process during digital investigations is staggering. From computers and mobile devices to cloud storage and IoT systems, investigators are tasked with sifting through massive amounts of data in search of critical evidence. With the increasing use of digital platforms, the scope of data has expanded beyond traditional sources, making it even more difficult to locate relevant information. This data overload—combined with limited personnel and budget constraints—challenges agencies to maintain efficiency and accuracy.

Furthermore, investigators must contend with more sophisticated encryption methods, advanced security protocols, and a variety of data sources. Traditional, manual methods of data extraction, analysis, and reporting are no longer sufficient to handle these challenges. These methods are not only time-consuming but also prone to human error, which further complicates investigations.

The need for modern, automated solutions that can streamline data processing and ensure accuracy is now more critical than ever. By automating repetitive tasks, investigators can save a substantial amount of time, freeing them up to focus on the more complex and critical aspects of an investigation. This allows them to apply their expertise where it truly matters, ultimately leading to more efficient use of resources and faster case resolutions.



How Magnet Forensics can help

With an estimated 90% of cases now involving a digital element that could be critical as evidence in an investigation, agencies need to embrace the power of digital forensics to operate efficiently, uncover crucial evidence, and build strong cases for prosecution.

Magnet Forensics allows agencies to seamlessly connect not only the hardware and software used by the digital forensics lab, but also digital evidence case management and collaboration between the various stakeholders.

Our tools streamline data collection, enhance investigative accuracy, and improve overall response times.

Overcoming encryption barriers

Magnet Graykey, a leading mobile forensics solution, allows investigators to bypass encryption on both iOS and Android devices. By gaining access to data locked behind encryption and security features, agencies can recover critical evidence—including messages, call logs, location data, and application history—that would otherwise remain inaccessible.

Advanced data acquisition and analysis

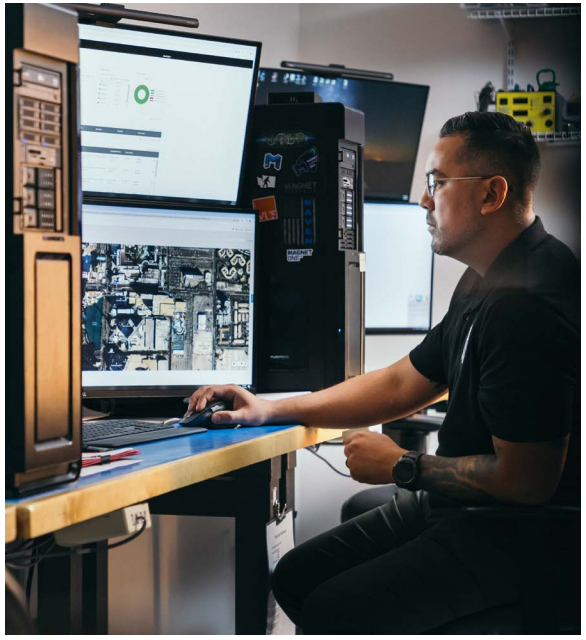
Tools such as Magnet Axiom and Magnet Axiom Cyber provide investigators with the ability to quickly acquire data from a wide variety of sources, including computers, mobile devices, and cloud storage. These tools can handle large datasets, enabling agencies to sift through vast amounts of evidence to identify key information and draw connections across different devices and platforms.

Efficient collaboration and review

The complexity of modern investigations often involves multiple investigators working on the same case. Magnet Review provides a collaborative platform where team members can securely access, annotate, and review evidence simultaneously. This secure, centralized approach to evidence management speeds up the review process and ensures all team members are aligned in their investigative efforts.

Comprehensive incident response

Modern digital forensics tools like Axiom and Axiom Cyber are designed to provide a comprehensive response to cybersecurity incidents. These tools enable investigators to track the full scope of an attack, identify the initial point of compromise, and trace cybercriminal behavior across multiple devices and systems. With these capabilities, federal agencies can quickly respond to breaches and mitigate any potential damage.



Strengthening agencies with advanced digital forensics tools

Magnet Forensics offers a full suite of powerful digital forensics tools which can help U.S. federal agencies effectively address critical challenges in modern investigations, from advanced cyber threats to overall efficiency in complex investigations. Our solutions streamline the process of securing sensitive data, enhancing incident response, and ensuring compliance with strict regulations.

MAGNET GRAYKEY™

Magnet Graykey is the leading mobile forensics tool designed to bypass security features such as encryption on iOS and Android devices. It enables federal investigators to access critical data—including messages, call logs, application data, and location history—from locked or passcode-protected devices. Graykey is an essential tool for investigating mobile-related crimes and insider threats, as it allows agencies to recover crucial evidence that may otherwise be inaccessible.

MAGNET GRAYKEY FASTRAK™

Graykey Fastrak allows you to unleash the power of your Graykey device at scale with a solution for extracting data from multiple mobile devices simultaneously. Pull more data in fewer steps with the most complete dataset available, directly to the examiner's workstation, accelerating data retrieval and streamlining your existing workflows.

MAGNET AXIOM®

Magnet Axiom offers a comprehensive solution for data acquisition, analysis, and reporting. It enables federal agencies to quickly and efficiently collect evidence from computers, servers, cloud environments, and network shares. Axiom allows investigators to analyze vast amounts of data, uncover hidden files, and correlate digital evidence across multiple sources. This powerful tool is essential for responding to a wide variety of cyber incidents and digital crimes.

MAGNET AXIOM CYBER™

Magnet Axiom Cyber is tailored for cybercrime investigations, particularly those involving advanced persistent threats (APTs), data breaches, and large-scale cyberattacks. Axiom Cyber enables investigators to analyze data across complex systems, including cloud environments and network traffic. Its ability to handle large datasets and track attacker behavior helps agencies identify the source of breaches and mitigate any future risks.

MAGNET REVIEW®

Magnet Review enhances collaboration during investigations, allowing multiple team members to securely access and review evidence in real-time. It simplifies the process of tagging, annotating, and organizing data, enabling faster analysis and more efficient case resolution. Review is crucial for maintaining a seamless workflow and ensuring investigative teams stay on the same page throughout complex cases.

MAGNET AUTOMATE™

Magnet Automate enables investigators to automate repetitive tasks such as data extraction, processing, and report generation. By eliminating manual steps, Automate allows teams to focus on higher-level analysis and decision-making. This tool helps federal agencies handle large volumes of data more efficiently, speeding up investigations and improving the accuracy of results.

MAGNET GRIFFEYE™

Magnet Griffeye empowers investigators to quickly process and analyze vast amounts of images and videos using advanced analytics and collaborative features. Designed for efficiency, it simplifies large-scale media forensics and streamlines digital investigations. The open, modular platform supports seamless integration with external tools, flexible workflows, and scalable data processing—giving you the adaptability and speed needed to stay ahead.

Conclusion: Key takeaways

Modern digital forensic tools like Magnet Axiom, Axiom Cyber, Graykey, Graykey Fastrak, Review, and Automate provide essential solutions to the challenges of digital investigations.

By improving data acquisition, overcoming encryption challenges, facilitating seamless collaboration, and automating routine tasks, these tools enable federal agencies to conduct faster, more precise investigations. In an era of rapidly evolving technology and increasingly sophisticated criminal tactics, modern digital forensic solutions are essential for ensuring investigative success and upholding national security.

Magnet Forensics empowers investigative teams to quickly and easily find, acquire, and share digital evidence across a diverse set of data sources with modern solutions. With Magnet Forensics, you'll benefit from the power of:

Integrated, intuitive, and easy-to-use solutions

We don't want digital investigations to slow down the pursuit of the truth. Our products make investigations more efficient—without compromising precision—so investigators can act quickly and decisively to help safeguard your agency.

> "The evidence shows what they did and what they know. We explain that we use the same process as the government and that we can prove whether there was hacking, malware, or some other way the material got on the system."
>
> —
>
> **Troy Schnack**
> Forensic examiner,
> United States Federal Public Defender
> for the Western District of Missouri

We collaborate with our customers

Magnet Forensics has developed a strong reputation in the digital forensics and cybersecurity communities with reliable products that respond to the evolving realities of our customers. We listen. Feedback is critical to fueling our innovation. We regularly engage with our customers, holding meetings and discussions to gather invaluable feedback, in addition to Product Advisory Councils—an exclusive forum to exchange ideas, insights, and feedback with our product management team to influence roadmaps.

> “One of the things that’s different with Magnet is, I think, personal connection with the user.”

Brett Shavers
Digital Forensics Consultant,
DFIR Training

Industry-leading training and expert support

Complex investigations require more than just cutting-edge tools—they demand exceptional support. Our commitment to your success is reflected in our comprehensive support offerings designed to ensure you get the most out of our solutions. We offer courses in a variety of formats, allowing you to find the method, location, and pace best suited for you and your team.

Learn more

Magnet Forensics is a developer of digital investigation software that acquires, analyzes, reports on, and manages evidence from computers, mobile devices, IoT devices and the cloud used by over 4,000 public and private sector organizations in over 90 countries and have been helping investigators fight crime, protect assets and guard national security since 2011.

MAGNET FORENSICS®

To learn more about how Magnet Forensics can help you and your agency with your digital forensics investigations needs, please visit **magnetforensics.com** or contact **sales@magnetforensics.com**