



Digital Evidence

Enhancing public safety using digital investigative technologies

Major Cities Chiefs Association
Digital Evidence Working Group

October 2024



Table of Contents

Introduction.....	3
Executive Summary.....	5
Methodology.....	6
Key Recommendations.....	7
Core Capabilities.....	9
Changing Nature of Digital Evidence.....	14
Cellphones: The Impartial Digital Witness.....	16
Digital Forensics Workflow.....	18
Management, Leadership, & Oversight of Digital Forensic Units	22
Contemporary Personnel Considerations	24
DFU Synergy with Other Entities.....	32
Legal & Regulatory Considerations.....	34
Digital Evidence Management	41
Procurement and Budget Issues.....	42
Addressing Privacy & Civil Liberty Concerns	45
Faraday Room Example.....	48
The Impact of A.I. on Digital Investigations.....	49
Success Stories.....	51
References.....	54
Resources and Further Reading.....	56
Acknowledgements.....	57



Introduction

Digital evidence is now the cornerstone in many investigations, providing critical insights that were unattainable only a few years ago. Furthermore, digital evidence can provide a level of detail and precision that corroborates and even bolsters traditional forms of evidence. For instance, geolocation data from mobile devices can place a suspect at a crime scene with remarkable accuracy. Social media interactions can reveal networks and motives that might otherwise remain hidden.

Devices such as smartphones, tablets, wearable technology, inter-connected household devices, and other technology that store data have repeatedly been shown to hold evidence which is critical to solving crime. A murdered woman's Fitbit log and Facebook activity offered key evidence leading to the arrest of her husband who alleged she had been killed by a home intruder. During a spree of hate-crimes in Texas, four defendants used a dating app to lure, and brutally victimize at least nine people who were targeted for their sexual orientation.

Modernizing Investigations

The proliferation of modern technologies has exponentially increased the scope and complexity of digital evidence. This evolution has necessitated a corresponding development of more sophisticated forensic methodologies and spawned an industry catering to public safety's need to access data with tools intuitive enough to be used by the average user, but technically advanced enough to access and collect information from ever-more complex sources.

Modern digital forensics involves intricate processes such as data extraction, analysis, and interpretation from a multitude of devices and platforms. It requires an understanding of various operating systems, encryption methods, and data recovery techniques. The field has become a multidisciplinary domain, integrating aspects of traditional investigative practices, computer science, and cybersecurity. Hiring, training, and compensating dedicated, trustworthy people to do this critical work can be challenging.

The use of digital evidence in policing comes with many challenges. The sheer volume of data generated by our modern digital ecosystems can be overwhelming. It is not uncommon for some police agencies to have backlogs of hundreds of devices waiting to be processed. Excessive wait times for investigators to process evidence can affect issues related to data privacy, chain of custody, and legal admissibility. The time required to complete digital forensic examinations is dependent on electronic processes. There is no way to "work faster" without the appropriate tools to complete the analyses, and sufficient personnel who have the training to complete this specialized work.



Digital Evidence is Different

One cannot discuss police data without acknowledging the unique nature of the information agencies collect. The information that law-enforcement possesses is often uniquely sensitive, from the embarrassing private details of feuds between significant others, to the traumatic and deeply personal details of a sex crime. In the normal course of business, police departments collect intimate details of people's lives related to situations when they are perhaps most vulnerable.

Unfortunately, many agencies lack the technical solutions that reflect a commitment to safeguarding data in a manner that is commensurate with conventional evidentiary standards. Law enforcement must effectively safeguard people's most sensitive personal data if they are to maintain their trust. Failing to adopt practices and systems that safeguard digital evidence places an agency at significant risk, but often cannot be easily remedied due to budget constraints, competing agency priorities, political influences, and a general lack of awareness.

A Brief History of Digital Evidence

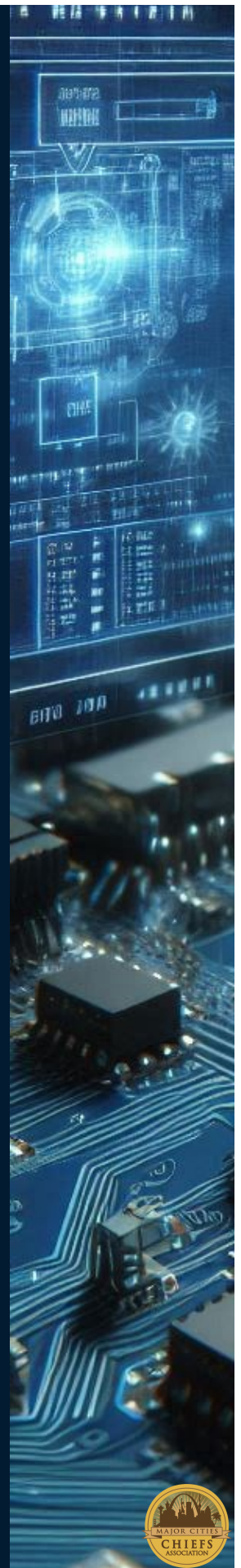
In the 1990's and early 2000's, cell phones were simple communication devices but still offered information such as call logs, contact lists, and rudimentary text messages, limited by both the number of allotted characters and a physical 12-button keypad.

Despite their simplicity, the information from such devices was still very valuable at the time, particularly in child exploitation cases, gang and street crime investigations, and other conspiracy-type offenses.

This time in history marked the beginning of a period that would see widespread adoption of personal computers and more advanced mobile phones.

The age of the internet brought about a new dimension of data, encompassing emails, web browsing histories, online communications, and eventually much more sophisticated devices offering apps which serve as portals to 3rd party messaging, social media platforms, encrypted cloud storage, and more robust location information.

Moreover, the emergence of the Internet of Things (IoT) has introduced an array of interconnected devices, including vehicles, smart home systems, wearable technology, and even appliances such as refrigerators and thermostats, all of which have the potential to yield data in an investigation.



Executive Summary

In October 2023, the Major Cities Chiefs Association (MCCA) launched a Digital Evidence Working Group composed of commissioned and civilian law enforcement personnel from multiple MCCA member agencies. The group's members have a wide range of expertise and span from investigators to bureau commanders and executive level managers. Each working group member is assigned to their agency's respective bureau that handles and examines digital evidence on a daily basis to solve various crimes.

This document is meant to equip executive police leaders with a sufficient understanding of the digital evidence landscape, enabling them to engage in more informed discussions with community members, elected officials, vendors, and other key stakeholders regarding the resources needed to realistically police in the digital age. The insights offered represent the collective work undertaken by a dedicated group of subject matter experts from across many MCCA member agencies. This collaborative effort identified a range of best practices, general guidance, and critical needs that have become essential in modern law enforcement.

This document discusses multiple topics surrounding the digital evidence landscape from the perspective of member agency investigators, examiners, and managers including the following; core capabilities, the changing nature of digital evidence, workflow, management, leadership, and oversight of digital forensic units, personnel considerations, DFU synergy with other units, legal and regulatory considerations, digital evidence management, procurement and budget issues, the impact of artificial intelligence, privacy and civil liberty issues, as well as success stories and lessons learned.

During the past 20 years, law enforcement has seen a remarkable evolution in how investigations are conducted, both in terms of the extent of information sources available, and with respect to the nature of the evidence required to secure a conviction in court. Much of this transformation has coincided with society's broader adoption of digital technology. In some ways, the rise of digital evidence is similar to the advent of fingerprint technology, and the integration of DNA profiling into criminal investigations. The key difference has been the speed and proliferation of digital evidence.

Today, nearly every investigation has some nexus to data, and almost every criminal case involves some form of digital evidence, whether the evidence is found in a smart phone, computer, tablet, vehicle, or any other electronic device. Handling and examining digital evidence is a capability that every law enforcement agency must be proficient in. This document will shine a light on how agencies today are routinely relying on data and digital evidence, as well as highlighting the challenges, benefits, and skills necessary to solve modern crimes in a ever evolving digital world.



Methodology

The MCCA Digital Evidence report serves as a comprehensive document that illustrates how member agencies use digital evidence to solve crimes through various methods, software, and hardware as well as current policies and procedures and outcomes of working with complex data during the course of investigations. The document contains twelve sections, individually authored by representatives from different member agencies, providing a more candid and personal approach to the reader. The following provides a short summary of each section:

Core Capabilities

The beginning of the document discusses the main purpose and basis of digital evidence, highlighting the difference between digital forensics and digital technologies as well as more detailed investigative techniques and procedures.

Changing Nature of Digital Evidence

The evolution of digital devices is explained, and how rapid technological advancements are influencing law enforcement's need to adapt their investigative techniques and expectations. Definitions pertaining to digital evidence are also provided.

Cellphones: The Impartial Digital Witness

This section describes how cell phones serve as silent digital witnesses—having the power to corroborate alibis, reconstruct sequences of events, and bring clarity to complex investigations, thereby ensuring justice without prejudice or agenda.

Digital Forensics Workflow

The fourth section focuses on business processes such as: case management, evidence handling and chain of custody, tool and technology management, examinations, documentation and reporting, and challenges and best practices.

Management, Leadership, & Oversight of Digital Forensic Units

Considerations when selecting supervisors and commanders for these specialized units is discussed in this section. The essential qualities of an effective digital forensics supervisor is also described.

Contemporary Personnel Considerations

The benefits and challenges of both civilian and sworn “specialists” in digital evidence units is described including training considerations, central operations vs. dispersed capabilities, and outsourcing certain tasks.

DFU Synergy with Other Entities

This section covers integrating tactics with investigative methods and how to effectively extract the data from a target device. It explains concepts such as “before-first-unlock” (BFU) and “after-first-unlock” (AFU) during cell phone extractions.

Legal & Regulatory Considerations

Ambiguous precedent case law and a lack of lawful access statutes currently affect digital evidence collection. There are also increasing limitations on the scope of digital search warrants, as well as technical challenges when extracting data.

Digital Evidence Management

Digital evidence is modernizing police investigations but data stewardship is paramount to effectively leverage it. This section discusses how data should be securely handled and stored.

Procurement & Budget Issues

Digital evidence personnel are constantly vetting the best tools available from multiple vendors and assessing current products as supervisors work through technical challenges with SaaS model products, licensing, and subscriptions.

Addressing Privacy & Civil Liberty Concerns

The sheer amount of digital data in modern criminal cases requires navigating the complex issue of privacy laws.


The Impact of A.I. on Digital Forensics

The age of deepfakes and other challenges associated with A.I. create challenges in authenticating evidence.

Success Stories

Agencies share candid stories of how digital evidence helped their investigators solve complex cases.





Key Recommendations

The proliferation of digital technology has fundamentally transformed the way that law enforcement investigates cases and safeguards the communities they serve. Technology is now an element of even the most basic street crimes.

More than forty MCCA member agencies contributed their insights, expertise, and data to identify best practices to meet the growing challenges related to digital investigations. The following recommendations are essential to enhancing the capabilities of law enforcement agencies in handling digital evidence:

1) Prioritize Investing in Modern Digital Forensic Tools

A well-resourced agency staffed with dedicated talented people, using tools sufficient to conduct modern investigations, is far more likely to close a case and obtain a conviction in court than one that is not. Investing in digital investigative solutions is not something that might be good to do eventually; it is categorically imperative now. Every year that an agency fails to modernize their investigative capabilities, they fall that much further behind.

2) Traditional Staffing Models May be Insufficient

Technology doesn't replace trained professionals; it helps good people do their best work. It is essential that agencies employ and develop the skillsets necessary to lawfully collect, analyze, interpret and manage digital evidence. Hybrid staffing models that include both sworn and civilian personnel may provide greater flexibility, technical expertise and organizational continuity.

3) Develop Comprehensive Training Programs

Agencies should implement tiered training programs that provide both foundational and advanced skills to forensic examiners. This ensures that personnel remain competent in the latest digital forensic techniques.

4) Digital Evidence Management is Critical to Mitigate Risk

A robust framework for digital evidence management should be established, ensuring proper chain of custody, secure storage, and timely processing. This is critical in reducing the liabilities associated with improper evidentiary procedures.



Key Recommendations

5) Legal and Regulatory Challenges Continue to Evolve

Agencies must monitor developing legal standards regarding digital evidence, such as search warrant limitations and data privacy concerns. Compliance with new requirements is critical to ensure digital evidence is admissible in court.

6) Improve Interagency Collaboration and Information

Effective collaboration between digital forensic units, investigators, and prosecutors enhances the speed and accuracy of investigations. Agencies should adopt standardized practices to streamline the sharing of digital evidence.

7) Expand the Use of Cross-Case Analysis

The prevalence of digital evidence offers more opportunities to gather information but comes with the added burden of sifting through volumes of data. Leverage technology to detect patterns and connections across multiple cases.

8) Consider Privacy Concerns

Agencies must balance the need to collect and analyze digital evidence with the imperative to respect privacy and civil liberties. Adopting policies that safeguard sensitive personal data while maintaining investigative integrity is essential to preserving community trust.

9) Secure Adequate Funding and Resources

A survey of MCCA member agencies revealed that "cost" was the top issue that has precluded agencies from adopting modern digital investigative solutions. Leaders must be prepared to advocate for sufficient budget allocations to build and sustain the digital investigative needs of their agencies now, and for the foreseeable future. This includes funding for tools, training, staffing, and the infrastructure necessary to manage increasing volumes of digital evidence.

10) Prepare for the Threats and Opportunities that AI Brings

As artificial intelligence and deepfake technologies become more prevalent, authenticating digital evidence becomes more critical. AI also has the potential to assist examiners in conducting more thorough investigations and surface insights more efficiently.



Michael Garvey, PhD
Deputy Managing Director
Philadelphia Police Department

Digital technology has transformed law enforcement practices, enabling more efficient and effective crime-solving methods. Two primary approaches have emerged: digital forensics and investigative digital technologies from commercial-off-the-shelf (COTS) equipment. While both play vital roles, they differ significantly regarding standards, accreditation, and validation requirements. Therefore, it is crucial that law enforcement agencies take responsibility and are well-informed to distinguish between the two options, adopting the program or combination of programs that is best for their operational needs and resource requirements.

Digital Forensics

Traditional Forensic Science Approach to Digital Evidence

Digital forensics is a specialized field that involves recovering, analyzing, and presenting digital evidence in a legally admissible manner. It requires stringent adherence to industry standards and accreditation processes to ensure the integrity and reliability of the evidence. Such analyses are typically conducted in an accredited forensic laboratory within a single law enforcement organization or as part of a regional system, such as an FBI Regional Computer Forensic Laboratory.

- 1) **Accreditation and Standards:** Digital forensics laboratories must adhere to standards set by organizations such as the ANSI National Accreditation Board (ANAB), the NIST & DOJ Organization of Scientific Area Committees for Forensic Science (OSAC), and the International Organization for Standardization (ISO) (ISO/IEC 17025 and ISO/IEC 17020). These standards cover various aspects of forensic practice, including quality management systems, technical procedures, and competence of personnel.
- 2) **Validation and Verification:** The tools and methodologies used in digital forensics must undergo rigorous validation and verification to ensure their accuracy and reliability (NIST, 2014). This process involves systematic testing and documentation to demonstrate that the tools produce consistent and reproducible results. Often, forensic capabilities extend beyond commercial-off-the-shelf (COTS) products and may require extensive expertise in areas such as computer science and engineering.
- 3) **Chain of Custody and Legal Admissibility:** Maintaining a clear chain of custody is crucial in digital forensics. Every step of the evidence-handling process must be documented to prevent tampering or contamination. Adherence to these protocols ensures that the evidence can withstand legal scrutiny and be admissible in court. Additionally, many jurisdictions have adopted stringent rules on accepting laboratory or forensic reports that are not applied to other forms of investigative evidence. Therefore, agencies are cautioned in using terms such as laboratory, laboratory report, forensic report, and forensic science unless that agency has adopted the appropriate accredited system of a forensic laboratory.



Investigative Digital Technologies

Flexibility and Accessibility

In contrast to digital forensics, investigative digital technologies involve leveraging COTS equipment and software to recover evidence. These tools offer flexibility and accessibility in an operational environment, allowing agencies to quickly examine physical evidence such as smartphones and tablets for digital evidence; however, they may not always meet the stringent standards required for forensic analysis.

- 1) **Commercial Off-the-Shelf Equipment:** Investigative digital technologies often utilize COTS equipment, such as hardware and software designed to access digital devices and extract digital evidence. These tools are readily available and can be quickly deployed in various investigative scenarios.
- 2) **Ease of Use and Speed:** The primary advantage of COTS equipment is its ease of use and speed. Law enforcement officers can use these tools to quickly recover digital evidence without advanced forensic training or accreditation.
- 3) **Limitations and Challenges:** COTS equipment offers convenience but also presents limitations. These tools may not undergo the same rigorous validation and verification processes as forensic tools, raising concerns about the accuracy and reliability of the recovered evidence. Additionally, the lack of standardized protocols can lead to inconsistencies in evidence handling and documentation. Therefore, it is imperative that agencies implement these capabilities in a manner that complies with the field's best practices and policies.

Understanding the distinctions between digital forensics and the use of investigative digital technologies is crucial for law enforcement professionals. While digital forensics provides a rigorous framework for ensuring the integrity and admissibility of digital evidence, investigative digital technologies offer flexibility and accessibility for immediate investigative needs. Balancing these approaches requires careful consideration of the specific requirements of each case, the available resources, and the legal implications of the evidence-handling process.

While both digital forensics and digital investigative technologies are important in modern investigations of potential digital evidence, this proceeding section of this article focuses on some of the core capabilities of Investigative Digital Technologies. Specifically, device unlocking and encryption bypass, evidence detection, data extraction, reporting, and cross-case analysis are some of the core capabilities of any digital investigation.



Device Unlock / Encryption Bypass

Unlocking Digital Barriers: One of the primary challenges with digital evidence is accessing data on locked or encrypted devices. Encryption, while essential for protecting user privacy, poses significant hurdles for law enforcement. Criminals often use sophisticated encryption techniques to secure their communications and data, making it difficult for investigators to retrieve critical evidence.

Techniques and Tools: Investigators employ various methods to bypass encryption and unlock devices. Initial methods may include collection techniques to prevent the device from locking, obtaining consent from an authorized individual or digital service provider, or social engineering techniques to obtain passwords. However, often investigative technologies must be employed to bypass the passwords and encryption. Through COTS equipment, brute-force attacks or software vulnerabilities may be used to access the data. A brute-force attack, which involves systematically trying all possible combinations until the correct one is found, offers one such method. However, this technique can be time-consuming and is not always feasible with strong encryption. Another approach is exploiting software vulnerabilities that use weaknesses in the device's coding to allow access to encrypted data without needing a password.

Collaboration and Legal Considerations: In some cases, law enforcement agencies collaborate with authorized users or device manufacturers to gain access to locked devices, provided there is a legal framework supporting such cooperation. This collaboration often requires court orders or warrants, ensuring the process respects privacy rights and legal standards. In cases where investigative units must unlock the devices through other means, it is still critical that all legal authorities be obtained before exploiting the device. The balance between upholding individual privacy and ensuring public safety is a critical consideration in this aspect of digital investigation (Casey, 2011).

Evidence Detection

Identifying Digital Footprints: Once access to a device is secured, the next step is detecting potential evidence. Digital evidence can take many forms, including files, emails, logs, metadata, and internet browsing history. The challenge lies in sifting through vast amounts of data to identify relevant pieces of evidence.

Advanced Detection Techniques: COTS software and analytical tools have been developed to automate detection. Pattern matching and keyword searches are used to identify specific terms or patterns related to the investigation. Metadata analysis provides additional context, such as the creation and modification dates of files, which can be crucial in understanding the timeline of events. File carving, a technique that reconstructs files from fragments found in unallocated space on storage devices, may also be used.



Reporting

Compiling Findings

Once the data has been extracted and analyzed, the investigators or analysts assigned to the digital investigation compile their findings into a comprehensive report. This report is a crucial document that summarizes the evidence and provides a detailed account of the investigative process. This document is supported by examination records that may be subsequently requested during discovery.

Report Structure

A typical report includes an executive summary that outlines the key findings and their significance, a listing of the recovered evidence, and a methodology section that describes the tools and techniques used during the investigation, ensuring transparency and reproducibility. Detailed findings present the evidence in a structured format, often accompanied by visual aids such as charts and timelines. The interpretation of evidence links the findings to the investigation's context, explaining their relevance. Agencies may issue a comprehensive report or choose to issue separate reports, one for the recovery of evidence and others for the intelligence analysis conducted on linkages and connections.

Legal Considerations

Reports must adhere to investigative and legal standards to be admissible in court. This includes ensuring that the evidence was collected lawfully and that the report accurately reflects the findings without bias. The chain of custody documentation is often included to demonstrate the integrity of the evidence throughout the investigative process (Casey, 2011). As noted earlier, unless a forensic laboratory actually completed the examination and produced the report, the agency should refrain from titling any investigative findings as a "laboratory" or "forensic" report to avoid misleading the reader about the nature of the document. Forensic reports often have additional evidentiary or legal requirements.

Cross Case Analysis

Identifying Patterns

Cross-case analysis involves comparing and correlating data from multiple cases to identify patterns, connections, or recurring elements. This capability is particularly valuable in investigations involving organized crime, serial offenses, or cyber threats, where similarities between cases can provide critical insights. These more complex intelligence analyses require large-capacity storage systems, legal authority to analyze data beyond the primary investigation, and advanced intelligence software to assist the investigator or intelligence analysts.

Techniques and Tools

Data correlation involves identifying common elements across different cases, such as IP addresses, email addresses, texts, files, photos, or phone numbers. Pattern recognition algorithms can detect similarities in modus operandi, helping investigators or analysts link seemingly unrelated cases. Link analysis creates visual representations of relationships between different entities, facilitating a deeper understanding of complex networks. Timeline analysis can uncover chronological connections, revealing how different events or actions are related. Such analyses may be conducted within an investigative unit, intelligence unit, or through a collaboration with a regional fusion center.

Strategic Advantages

Cross-case analysis not only aids in solving individual cases but also helps develop strategic approaches to combatting recurring threats. For instance, in organized crime investigations, cross-case analysis can uncover the structure and operations of criminal networks, leading to more effective disruption strategies (Lillis, Becker, O'Sullivan, & Scanlon, 2016).

Conclusion

Investigative Digital Technology plays a pivotal role in modern law enforcement, providing the tools and techniques needed to uncover, analyze, and present digital evidence. The capabilities of Device Unlock / Encryption Bypass, Evidence Detection, Data Extraction, Forensic Reporting, and Cross Case Analysis are fundamental to effective investigations in the digital age. As technology continues to evolve, law enforcement agencies must remain adept at leveraging Digital Investigative Technologies and securing Digital Forensic capabilities, as needed, to address the challenges posed by modern crimes. By investing in training, tools, and collaboration, agencies can ensure they are prepared to navigate the complexities of digital evidence and uphold justice in an increasingly digital world.

FAQs

1. What is the primary goal of investigative digital technology? The primary goal of investigative digital technology is to collect, preserve, extract, and present electronic data in a legally acceptable manner to support investigations and legal proceedings.
2. How are encrypted devices unlocked? Investigative digital technology units may use COTS platforms to conduct social engineering attempts, brute force attacks, or exploit software vulnerabilities to unlock encrypted devices. If these methods do not work, evidence may be transferred for more advanced digital forensic examinations.
3. What types of digital evidence can be collected? Digital evidence can include emails, text messages, photos, videos, and metadata, among other forms of electronic data.
4. Why is formal reporting important? Formal reporting is crucial because it clearly organizes findings, which is essential for investigations and legal proceedings.
5. What is cross-case analysis in investigative digital technology? Cross-case analysis involves comparing data and evidence from multiple cases to identify patterns or connections that may indicate a larger criminal network. Once data is extracted from the digital device, investigators or analysts may use various methods, including COTS linkage analysis software, to identify trends and connections within the data.

Changing Nature of Digital Evidence

Lisa Merzski

Supervising Criminalist

San Diego Police Department Crime Laboratory

Almost everyone has a cell phone and that means criminals do as well. The nature of digital devices has evolved significantly over the years, driven by rapid technological advancements, and changing user needs. Technology has become integrated into our everyday lives. This means there is digital evidence in almost every criminal case. What are some of the key trends in the changing nature of digital evidence?

- 1) **Miniaturization and Portability** – the sheer number of different phones, computers, hard drives, thumb drives, drones, cameras, watches, and tablets seen by law enforcement require different tools to access. Even gaming systems such as PlayStation and Xbox can have valuable data.
- 2) **Connectivity** – devices are talking to each other. Ring camera videos can be in multiple locations. Smart home devices like Nest are interconnected with multiple devices in the home such as lights and appliances. Smart watches are sharing data with applications on phones and other devices. Connected cars communicate their locations. This also means there is data in the cloud from applications that are accessed by all these different devices.
- 3) **Artificial Intelligence (AI) and Automation** – AI like Siri and Alexa have become a core component of many digital devices. Sometimes these assistants can have key information on what a user has searched. There are also automated services they perform.
- 4) **Enhanced User Interfaces** – touchscreens and voice commands have made devices more user friendly. Facial recognition and gesture controls have replaced traditional passcodes on many devices.
- 5) **Storage** – the amount of data on these types of devices has substantially changed. That means the amount of time it takes to download a device has increased as has the amount of storage needed to house this evidence. The average digital device could have a Tera Byte (TB) of data. What does that translate to? A short book that is 100 pages is about 1-2 Mega Bytes (MB). A TB of data is equivalent to 500,000 books. A single criminal case could have 5 devices with this amount of data. Finding better solutions to store this data will be needed for the foreseeable future. Our modern society and criminals alike, are carrying an entire computer in their hand. These devices carry all the information about locations, purchases, photos, videos, music, and social media along with the people and places they interact with. It can take many, many hours to obtain the data from these devices. Law enforcement agencies used to purchase compact discs to store data from a criminal case. Agencies soon needed to purchase dual-layer blue ray discs, followed by flash drives of increasing size from 128 MB, 250 MB, 1 GB, and 1 TB. Now external hard drives are needed to store and read the data from a single mobile device or computer. Ideally, agencies should have a secure enterprise based storage option.

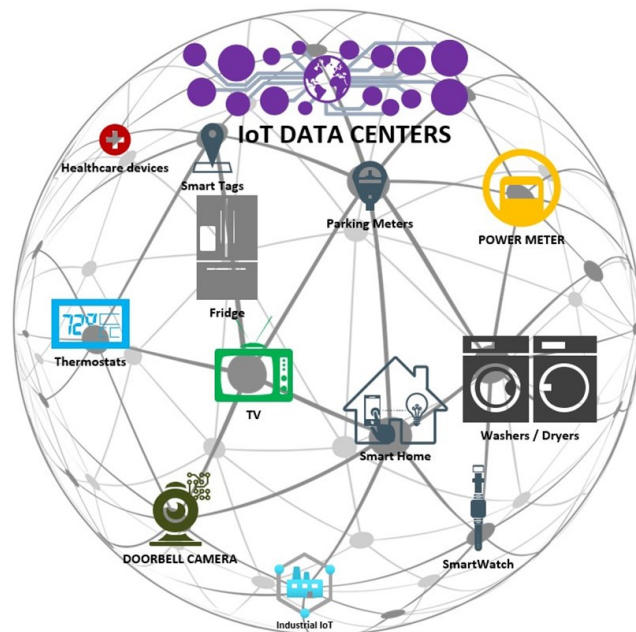
Memory Unit	Description
<i>Kilo Byte</i>	1 KB = 1024 Bytes
<i>Mega Byte</i>	1 MB = 1024 KB
<i>Giga Byte</i>	1 GB = 1024 MB
<i>Tera Byte</i>	1 TB = 1024 GB
<i>Peta Byte</i>	1 PB = 1024 TB

Changing Nature of Digital Evidence

Improved collaboration and information sharing – Law enforcement agencies are increasingly collaborating and sharing information. This helps standardize procedures and improve the overall effectiveness of digital evidence investigations.

Faraday boxes, bags, and rooms – because devices can be accessed in so many ways, making sure they cannot be accessed outside of a law enforcement agency is paramount. This means isolating the devices and digital evidence from the internet. There are several ways to do this, but one of the best ways is to place them in a faraday box or room which blocks external signals. This means a device cannot be remotely wiped by the user.

Passcode analysis – there are now advanced tools to find a passcode for a digital device. Law enforcement agencies worldwide are purchasing these tools to keep up with the ever-evolving digital landscape in our daily lives. Technology has enhanced convenience and overall user experience, but this also means law enforcement must adapt to that changing landscape.



Definitions

Android OS = Mobile operating system based on a modified version of the LINUX kernel and other open-source software.

AFU = After First Unlock (e.g., when a cellphone has been unlocked by the user and not turned off)

BFU = Before First Unlock (e.g., when a cellphone is off and turned on with no unlock code entered)

Cell Tower = An object with 3 panels per side, which includes a transmitter and two receivers.

CDMA = Code Division Multiple Access

Data = Information in analog or digital form that can be transmitted or processed.

GSM = Global System for Mobile Communications

Hard Drive = reference to hard drive disks (HDD) or solid-state drive (SSD) that stores data to a computing device.

Internet = The single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB) and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).

iOS = The operating system for Apple iPhones or iPads.

IoT = Internet of Things refers to a network of physical devices, vehicles, appliances, and other physical objects that are embedded with sensors, and network connectivity, allowing them to collect and share data.

Mobile Device = A portable device that has an embedded system architecture, processing capability, on-board memory, and may have telephony capabilities (e.g., cell phones, Global Positioning System (GPS) device, or tablets).

OS = Operating System

SIM Card = Subscriber Identity Module (e.g., card with a chip that is used to communicate between the cellphone and service provider)

VPN = Virtual Private Network



Cellphones: The Impartial Digital Witness

Kyle Dishko
Deputy Chief
Arlington Police Department

Christian Quinn
Managing Principal,
Fulcrum Innovation LLC

Cell phone data can provide invaluable insights into events, timelines, and personal interactions. Unlike human witnesses whose memories may be generally unreliable, or motivated to serve their own self-interests, the digital evidence stored on cell phones is factual, neutral, and precise. This is critical to ensure that the truth comes to light, whether it exonerates an innocent individual or provides critical evidence implicating the correct suspect.

In New Jersey, a witness placed a suspect at the scene of a homicide. Investigators obtained a search warrant for his phone. By analyzing the location data, investigators corroborated the subject's original alibi, determining that he was in fact in another state at the time of the murder. By ruling out the original suspect, investigators were able to focus on identifying people and evidence that were actually pertinent to the case.

In an unrelated investigation, New Jersey law enforcement officers received a report from a woman who alleged that her former domestic partner was sending her threatening text messages in violation of a restraining order. At first glance, it appeared that the messages had been sent to her. However, upon examining the alleged suspect's phone, they found no evidence to substantiate that the suspect sent the messages. A deeper examination of the alleged victim's phone revealed that she had actually manipulated the contact information for the suspect and had been sending herself the text messages.

The San Diego Police Department investigated a case involving the possession of child sex abuse material. While an explicit image was in fact located on the subject's device, examiners determined that the image was located in conjunction with malware that had been attached to the suspect's download from a website where one would not expect to download child sex abuse material. Their investigation determined that the subject did not intentionally or knowingly download the unlawful content.



Cellphones: The Impartial Digital Witness

By serving as a silent digital witness, cell phones have the power to corroborate alibis, reconstruct sequences of events, and bring clarity to complex investigations, thereby ensuring justice without prejudice or agenda.



On September 21, 2023, a motorcyclist was killed in a fatal hit and run crash outside Dallas, Texas. With little information to follow-up on, detectives developed a strategy to identify cellular devices around the crash. This required using cell-site location information from multiple towers to identify any devices that could have been in the area at the time of the event.

Detectives identified a device belonging to subject from Mississippi who was on parole and not supposed to be out of the state of Mississippi. During a subsequent interview, the subject told police that he was a passenger in the vehicle and named a second suspect as the driver who ran over and killed the motorcyclist.

The second suspect was uncooperative and denied being the driver of the vehicle, only stating that he was asleep at the time of the crash. Additional digital forensic examinations were conducted. Investigators discovered information that the original subject was driving, and the second subject was in the vehicle, but he was asleep in the backseat at the time of the fatal crash confirming what he told officers.

The original suspect was confronted and confessed that he was driving and was charged for the crime. Investigators learned that the involved vehicle was taken to Dallas where it was scrapped and disposed of in a car crusher. The digital forensic examinations exonerated the second subject and implicated the first subject who had falsely accused him. Without digital forensic tools and the dedicated work of the involved detectives, the wrong person could have been charged for this crime.



Capt. Aaron Busch
Lt. Max Watson
J. Bret Aicher
Michael Pickle
Austin Hartzler



Oklahoma City
Police Department

Digital forensics, a specialized branch of forensic science, delves into the recovery and investigation of material found in digital devices involving the application of analytical and investigative techniques to recover and analyze data. Digital forensics encompasses a broad spectrum of devices and data types. Common targets of investigation include computers, smartphones, tablets, servers, and even cloud-based storage systems. The data recovered from these devices can range from pictures and videos, to emails and documents, as well as internet browsing history, deleted files, and even hidden data.

As our world becomes increasingly reliant on technology, the importance of digital forensics has grown exponentially.

The goal is to preserve, identify, recover, analyze, and present facts about the information found in electronic evidence. The digital forensic business process underpins investigations, emphasizing their importance in maintaining the integrity of evidence and ensuring the successful resolution of cases.

Digital forensics investigations require well-defined business processes to ensure efficiency, accuracy, and compliance with legal standards. These processes encompass various aspects of the forensic lifecycle. A digital forensic investigation typically follows a systematic approach.

1) Case Management

Effective case management is crucial for tracking the progress of investigations, managing evidence, and coordinating with law enforcement agencies. The initial phase involves recognizing the potential existence of digital evidence and identifying its location. This stage requires a clear understanding of the case objectives and potential sources of digital information.

Key elements include:

- Case intake and assessment
- Search authority (search warrant/search waiver)
- Case assignment and resource allocation
- Evidence chain of custody
- Communication and collaboration
- Case closure and archiving



2) Evidence Handling and Chain of Custody

Maintaining the integrity of evidence is paramount. Preserving digital evidence is critical to maintain its integrity and admissibility in legal proceedings. This involves creating exact copies of the original data, using forensic imaging techniques, and storing them in secure environments. Acquiring digital evidence from various sources, including computers, mobile devices, servers, and network infrastructure. This process demands specialized tools and techniques to extract data without altering the original evidence.



3) Tool and Technology Management

Digital forensics relies heavily on specialized tools and technologies. The common tools used in examining computers are Magnet AXIOM, FTK (Forensic Toolkit), FTK Imager, Encase, Forensic Explorer, and Autopsy.

The tools most commonly used to extract data from mobile devices are Cellebrite Premium, GrayKey, XRY, and Datapilot.

Investigating data on mobile devices also presents its challenges. Devices may be in a locked or unlocked state. The passcodes to unlock the devices might not be known or given. The power status of the mobile device might affect how much data can be recovered from the phone. The phone could be in an after-first-unlock (AFU) which could provide more data as where a phone in a before-first-unlock (BFU) mode might not provide as much data.

Berla is a widely used tool in vehicle forensics. Vehicles hold a vast amount of data that can be used to uncover critical information during an investigation and help determine what happened, where it occurred, and who was involved.

Effective management of hardware and software resources involves:

- Tool selection and evaluation
- Software licensing and maintenance
- Tool calibration and validation
- Regular updates and upgrades



4) Examination

Collected data undergoes a thorough examination to identify relevant information. Analysts and investigators use specialized software to extract, analyze, and interpret data, looking for patterns, anomalies, and evidence that supports or refutes the investigation's hypotheses. The analysis phase involves interpreting the examined data to draw conclusions and develop investigative leads.

A digital forensic investigation typically follows a methodical approach:

Acquisition: The initial step involves creating an exact replica of the digital device or storage medium. This process, known as imaging, ensures that the original data remains unaltered while investigators work with a copy. This process demands specialized tools and techniques to extract data without altering the original.

Identification: Once an image is obtained, analysts and investigators identify relevant files and data for further examination. This may involve sorting through vast amounts of information to pinpoint specific items of interest.

Analysis: The identified data is meticulously analyzed to extract meaningful information. This phase often requires specialized tools and techniques to recover deleted files, decrypt encrypted data, and reconstruct events. The collected data undergoes a thorough examination to identify relevant information. Analysts and investigators use specialized software to extract, analyze, and interpret data, looking for patterns, anomalies, and evidence that supports or refutes the investigation's hypotheses.

Interpretation: The findings from the analysis are interpreted within the context of the investigation. Forensic experts draw conclusions based on the recovered data, providing valuable insights to legal teams.

Ensuring the accuracy and reliability of forensic findings is essential. Quality assurance and control processes include:

- Standard operating procedures
- Internal audits and peer reviews
- Proficiency testing
- Certification and accreditation



5) Documentation and Reporting

Comprehensive and accurate documentation is vital for legal proceedings and internal review. The final stage involves documenting the findings in a clear and concise report. The report should be comprehensive, accurate, and understandable to legal and non-technical audiences. It may include detailed descriptions of the investigation process, methodologies used, evidence collected, and analysis results. Throughout the investigation, detailed documentation is maintained. This includes chain of custody records, analysis reports, and any other relevant information. Accurate documentation is essential for ensuring the admissibility of evidence in court.

Documentation and reporting encompass:

- Report templates and formats
- Evidence documentation standards
- Report review and approval
- Report dissemination and storage

Challenges and Best Practices

Digital forensics practitioners face numerous challenges, including the increasing complexity of digital systems, the evolving nature of technology, and the need to balance efficiency with accuracy. Digital forensics is a dynamic field constantly evolving to keep pace with technological advancements. Some of the key challenges faced by forensic investigators include:

- Data Volume: The sheer volume of data generated by modern devices can be overwhelming. Efficient data management and analysis techniques are crucial for timely investigations.
- Data Volatility: Digital evidence can be easily modified or deleted. Rapid response and advanced data recovery techniques are essential to preserve critical information.
- Encryption: Increasingly sophisticated encryption methods can hinder access to valuable data. Forensic experts must stay updated on the latest encryption technologies and develop countermeasures.
- Cloud Computing: The proliferation of cloud-based services presents new challenges for digital forensics. Investigators must understand the complexities of cloud infrastructure and data retention policies.

To address these challenges, organizations should adopt best practices such as:

- Staying Updated: Keep abreast of the latest forensic techniques, tools, and legal developments.
- Continuous Training: Provide ongoing training to forensic analysts to enhance their skills and knowledge.
- Collaboration: Foster collaboration among forensic teams and with other stakeholders.
- Standardization: Implement standardized procedures and workflows to ensure consistency.
- Data Security: Protect sensitive data and maintain confidentiality.
- Ethical Considerations: Adhere to ethical guidelines and professional standards.

Conclusion

Digital forensics is a complex and critical field demanding rigorous business processes to ensure the integrity of evidence and the successful resolution of investigations. By implementing well-defined procedures for case management, evidence handling, tool management, quality assurance, and documentation, forensic organizations can enhance their efficiency, accuracy, and credibility. As technology continues to evolve, the importance of robust business processes in digital forensics will only increase.

Management, Leadership, & Oversight of Digital Forensic Units

Major Brendan Hooke
Assistant Commander
Fairfax County Police Department

When selecting a supervisor for a digital forensics team within a law enforcement agency, it is crucial to recognize the unique demands and challenges of this specialized field. Agencies must first define the type of unit they intend to staff and establish corresponding expectations. Some agencies opt for a full-scale digital forensic lab, while others prefer a less technical, field-based unit. Understanding the unit's purpose is essential for managing expectations, guiding procurement decisions, and, most importantly, staffing appropriately.

Drawing from my experience as the inaugural digital forensics supervisor for the Fairfax County Police Department's Digital Forensics Section, I have witnessed the transformative impact of focused and skilled leadership. In today's rapidly evolving digital landscape, a digital forensics unit requires a supervisor with a robust blend of technical expertise and leadership skills, who also serves as an advocate, gatekeeper, evangelist, and motivator. Such a leader ensures that the team remains aligned with agency goals, upholds high standards of forensic integrity, and adapts to the ever-changing technological environment. This essay outlines the essential qualities of an effective digital forensics supervisor, emphasizing the need for a process-oriented, visionary, communicative, and organized leader to guide the team to success.

Varied Experience

A leader in a digital forensics team must have a blend of investigative, operational, and administrative experience to navigate the multifaceted responsibilities of the role effectively. While prior technical experience is advantageous, the ability to learn and apply technical concepts in operational contexts is even more critical. A well-rounded supervisor who understands investigative techniques, operational workflows, and administrative procedures can bridge the gap between technical specialists and law enforcement objectives. This adaptability enables the supervisor to support their team in delivering precise and timely forensic results. Agencies must also determine whether they expect their supervisors to actively participate in forensic examinations and, if so, to what extent. Balancing supervisory duties with hands-on involvement in forensic work will depend on the agency's specific needs and the supervisor's capacity to manage both roles efficiently.

Process-Oriented

A process-oriented leader is essential for establishing and updating the policies and procedures necessary for a digital forensics section to meet the growing demand for its services. By creating clear and efficient processes, the leader ensures that resources are utilized effectively and provides a structured framework that guides the team's efforts. This structured approach helps manage the often overwhelming workload, preventing the team from being derailed by urgent issues and maintaining a consistent, orderly workflow. Moreover, well-defined processes allow requesting entities to understand what to expect, fostering transparency and reducing wasted time and resources. Through diligent policy and procedure management, the leader can create a resilient, adaptive, and efficient digital forensics section that meets high demands.



Management, Leadership, & Oversight of Digital Forensic Units

Visionary

The digital investigations landscape is rapidly evolving, requiring a leader who can anticipate challenges several years in advance, including technical, legal, and operational issues. Once these challenges are identified, the leader must develop several strategies to address them. For example, if an Apple iOS update temporarily disrupts commercially available anti-encryption devices, the unit leader should have a plan for lawful access to encrypted phones. A visionary leader's response should include a blend of social engineering techniques, communication strategies for operational units to preserve access, and a plan to use lawful alternative technical methods.

Communicator

Advanced digital evidence capabilities are of little use to an agency if no one outside the unit understands them. Perhaps the most essential skill for a leader in this role is the ability to explain technical material to a non-technical audience and articulate its impact on operations, investigations, or overall agency strategy. During my time as a Digital Forensic Section leader, I regularly updated my investigative counterparts about the current state of iOS technology, enabling them to plan investigative strategies that prioritized seizing cell phones in the best condition possible (before first unlock). During a homicide investigation, detectives remembered our advice on preserving evidence on a suspect's cell phone.

They surveilled the suspect, called him to get him to unlock the phone, and took him into custody while he was on the phone. The unlocked phone was quickly transported to our Faraday room in the digital forensics unit, leading to the recovery of the victim's body and the conviction of the suspects. In this case, communication was vital in helping detectives formulate a winning strategy.

Organized

A well-run digital forensics unit requires active case management to screen and prioritize incoming cases, ensuring that valuable resources are used efficiently. Every case is a priority for the requestor, but the leader must keep an eye on the big picture and ensure that case resources align with agency priorities. Identifying and analyzing these priorities is easier when the leader can quickly assess the unit's current workload, backlog, and pending requests. Effective execution and gatekeeping rely on articulated policies, procedures, and systems; allowing personal relationships or urgent issues to dictate case management frustrates digital forensic examiners and wastes resources. Organization is a critical skill not only for case management but also for administrative management. Most units require numerous resources, including hardware, software, and training. The unit leader must ensure that budgets, contracts, and certifications are always up to date to prevent the agency from losing access to valuable resources.

Succeeding as a Digital Forensics Leader

Congratulations on being selected to lead a digital forensics unit. Here are some concepts and resources that will help you succeed:

- 1) Seek a Role Model or Mentor: I found leaders in similar roles at nearby agencies and actively sought their advice. Understanding their challenges and learning from their experiences helped me excel.
- 2) Network with Other Leaders: The "nerd cop" space is a tight-knit community. Networking with other leaders will help you learn how they solve the same problems you face. It also reassures you that you are not alone in facing these challenges. Additionally, they likely share your passion for digital forensics and will enjoy discussing the field with you.
- 3) Pursue Formal Training: Formal training can help hone your skills. Attend technical training to better understand your examiner's perspective. The International Association of Computer Investigative Specialists offers a *Managing a Digital Forensics Lab* class that provides excellent value.



Contemporary Personnel Considerations

Kate Rosoff

Forensic Specialist Supervisor
Albuquerque Police Department

Most frequently, digital evidence units are staffed with sworn personnel, rather than civilians. There are benefits and drawbacks to each, but both sworn and civilian units face staffing issues based on turnover, often due to a lack of opportunities for advancement for both sworn and civilian examiners.

Staffing Challenges: Sworn vs. Civilian

Sworn Units

Units staffed with sworn forensic examiners often face challenges with turnover. In many departments, officers must leave the unit in order to be promoted. Other departments require that officers be reassigned after being in the same position for several years. This means that training resources are regularly required to ensure that new forensic examiners maintain the same standard of work when officers leave the unit.

Many police departments are also experiencing personnel shortages, and positions that take officers out of the field are often not prioritized.

Several units have recognized the benefit of maintaining continuity in their digital evidence unit staff and have developed an internal promotion process.

In many departments, the digital evidence positions are highly coveted. It's a difficult unit to join, and those who join the units often stay for the remainder of their careers.

Training in digital evidence allows officers to access new opportunities for training and development, with many of the learned skills transferring to job opportunities when the sworn staff retire from law enforcement.



Contemporary Personnel Considerations

Civilian Units

Digital evidence units that are staffed with civilians can be beneficial when facing challenges stemming from sworn position vacancies. Civilians who already possess essential training and education can be hired into forensic positions, allowing them to be more technically effective sooner. Training forensic examiners is time and resource intensive, whether civilian or sworn.

There are several challenges to maintaining a civilian workforce. Because many departments have not developed a clear path for career advancement for civilian personnel (in terms of increases in pay and/or responsibility), departments report having civilians leave for more highly-paid, private sector jobs after having completed training. This is particularly problematic in geographic areas where technical skillsets are in high demand.

There can be challenges with trust between sworn and civilian staff. In many instances, sworn personnel prefer to keep details of their investigations to themselves, which poses a problem for a forensic examiner assigned to assist with an investigation.

These challenges can be overcome when detectives understand the value that civilian examiners can add by relieving the detectives of some of their workload and when trusting relationships are built between sworn and civilian co-workers.

Hybrid Units

Several units also have hybrid teams, with civilians handling some duties, while sworn officers handle others. Several agencies described policies within their agencies or legal landscape that prevent civilians from handling search warrants or certain types of evidence, particularly evidence that might contain Child Sexual Abuse Material (CSAM).

As digital evidence continues to increase in importance, agencies will have to grapple with the challenges that exist in maintaining a workforce, whether sworn or civilian.

Out of **35**
MCCA Member Agencies:

Only **Sworn/**
Commissioned
personnel are
dedicated to digital
forensics

22

Hybrid units with
both
sworn and civilian
personnel

11

Only have **Civilian**
personnel
dedicated to
digital forensics

3

Agencies with
Forensic
Scientists/
Examiners

13



Contemporary Personnel Considerations

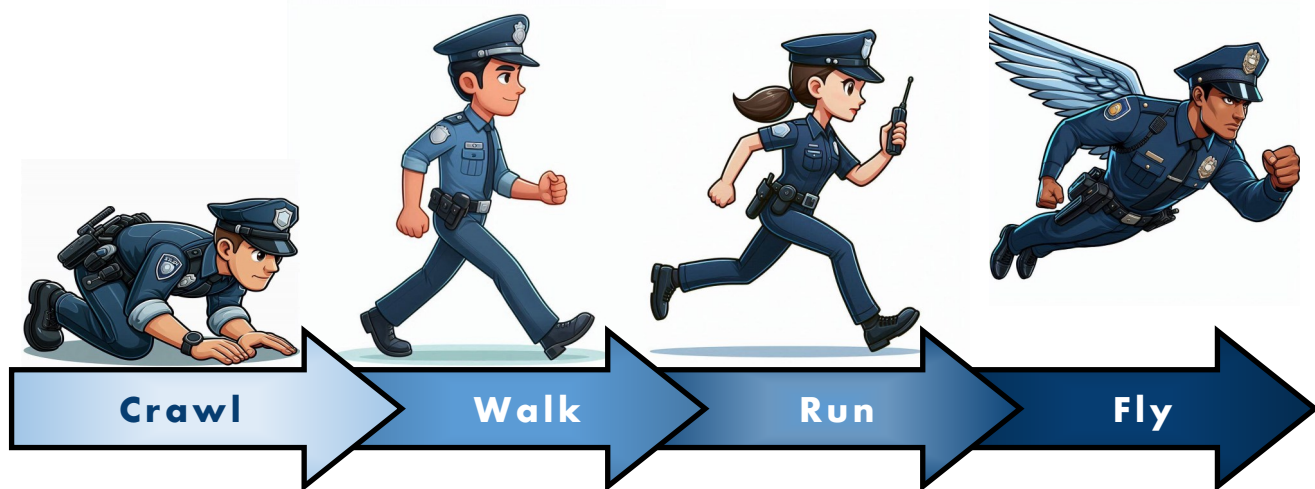
Zachary Johnson
Commissioned Supervisor
Digital Forensics Lab

Las Vegas Metropolitan Police Department

Specialist Training in Digital Forensics

Taking a skilled law enforcement officer and providing them with the training necessary to become efficient in the field of digital forensics, makes them a powerful tool when the need arises to properly handle digital investigative technologies. This skillset is not acquired overnight, however, and the amount of information needed can be overwhelming at times.

Tasking an employee to “learn” digital forensics for law enforcement purposes is different than taking a detective skilled in the investigation of robberies and asking them to now investigate homicides. The skills learned in the police academy, field training, and experiences on the beat, make employees experts in the rules of search and seizure, how to conduct an investigation, and the evidence needed to prove the innocence or guilt of a person. But that training is only a baseline for what is needed for a person who identifies, preserves, collects, analyzes, and testifies about digital evidence. The digital crime scene requires a new level of training that is constantly changing and moving. National recognized training standards for digital investigators does not currently exist. There is a patchwork of certifications and training offered by a variety of federal agencies, private sector companies, and other law enforcement groups.



Lets Learn to Crawl Before We Run

A tiered approach to training is very beneficial to acquire the knowledge necessary to tackle digital technology and to be able to contribute to investigations as you are learning. When an employee is now responsible for the digital crime scene, they must learn to crawl before they walk, and walk before they run. Eventually they will be able to fly but let's talk about how you can help them get there. Whether you have a seasoned and well-educated staff in your digital forensics lab or are new to the digital forensics field, all new employees must start somewhere. There are several sources that can fulfill your training needs.

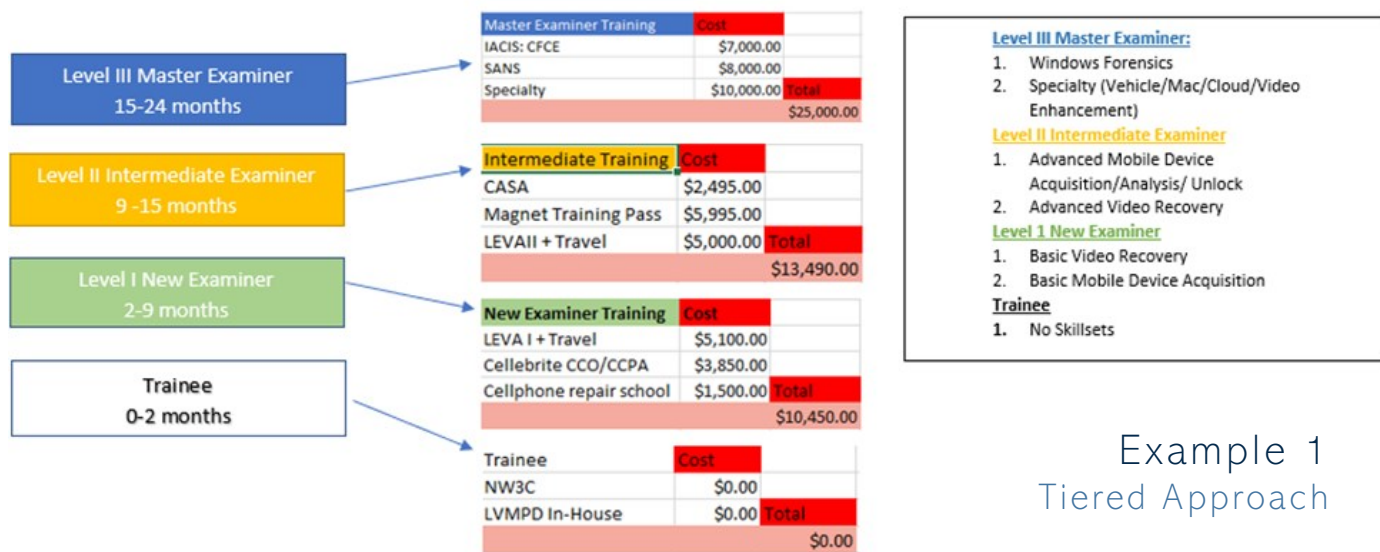
They include:

- Digital Forensic Tool Vendors for: Cellphone, Computer, Video, Vehicle
- Agnostic Tool Training Companies
- Federal Counterparts such as: United States Secret Service National Computer Forensic Institute



Contemporary Personnel Considerations

With so many choices, you want to ensure your employee begins by receiving training in the tools they are using. Once they master the basics, they can progress to topics such as advanced cellphone repair and SQL database courses.



Example 1
Tiered Approach

This tiered approach allows new employees to begin basic video collection in as little as 2 months after transferring to digital forensics and basic cellular phone extractions within 6 months. Prior to being authorized to complete video recovery, cellular phone examinations, or computer examinations, several peer review sessions should take place to ensure the forensic methods and work product of the new employee conform to your department standards.

New employees master a series of smaller digital forensic related topics instead of becoming overwhelmed with a flood of information. At the completion of Level III Master Examiner, a specialty may be selected by the new examiner to master further. These specialties can include vehicle forensics, Linux forensics, and Mac forensics among others.

An agency should evaluate their needs when dealing with the digital crime scene. What services do you want to offer in-house, and what services might you outsource. The services provided in-house will be limited by budget, staff, and skillsets.

Some common services offered in-house are:

- Mobile device forensics
- Computer forensics
 - * Windows/Apple/Linux
- Video collection
- Vehicle forensics
- Specialties
- Device repair
- Deleted data recovery

Training Costs

Adding digital forensics to your toolbelt is not cheap, and neither is the necessity to properly train your employees. A tiered approach to training adopted by your agency can provide a financial roadmap to how much each new employee added to the unit will cost over time. This cost is not a singular investment. It is an investment that must be replenished year after year to ensure certifications for courtroom testimony are maintained and that your employees are up to date on emerging digital technologies.



Contemporary Personnel Considerations



Points to Consider

Training should be delivered in a tiered approach and focused on learning one category at a time so that the employee does not become overwhelmed.

Training should be sought from credible industry providers and complement the tools you plan to outfit your employees with. Depending on your jurisdiction, certifications from training providers regarding the tools you use may be necessary to offer courtroom testimony.

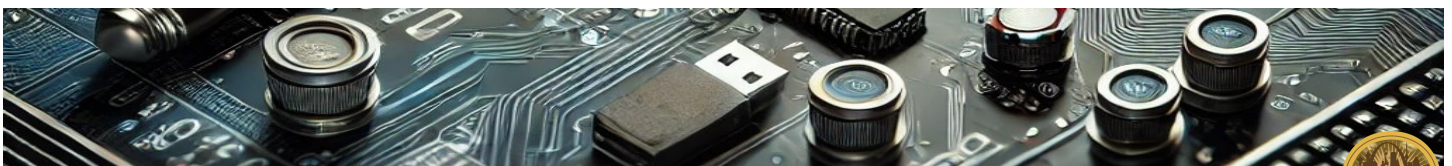
Certifications require continuing professional education credits (CPE's). Your budget should reflect the need to continually provide training to your employees. In addition, new and emerging digital technology, tools, and skills are constantly emerging that require the continual education of your employee.

Once basic skillsets are acquired, your agency can focus on more advanced training to include advanced device repair, advanced mobile device forensics, and vehicle forensics.

Central Operations vs. Organizationally Dispersed Capabilities

As more and more law enforcement agencies across the United States include digital forensics as a tool in their toolbox, we are always looking for better and faster ways to get the same job done. There are many things you should give thought to when considering to organizationally disperse your digital forensic capabilities across your department. There are a few things to consider when evaluating if a centralized or dispersed digital forensics model is right for you.

A digital forensics lab and its employees are responsible for the identification, preservation, collection, analysis, and ultimately the testimony regarding digital evidence. The lab handles both physical and digital evidence. The integrity, confidentiality, and chain-of-custody of that evidence is of utmost importance. Maintaining a controlled environment is essential for maintaining the confidentiality of high-profile events and integrity of sensitive data that will pass through.



Contemporary Personnel Considerations

Centralized Location

Many agencies have at least some level of digital forensics capabilities. They may have one to five detectives assigned to complete the digital forensic needs of their entire agency. These detectives have developed a set of skills that makes them unique amongst their peers. These skills need continual training and access to specialized hardware/software that can be financially costly to the agency.

Keeping these employees in a central location may allow them to utilize the same software and hardware which could reduce the operating costs of their unit. Adding additional hardware and/or software may be used as a force multiplier instead of hiring an additional employee. A single employee can have multiple pieces of evidence processing at the same time if they have the tools available to them.

Benefits

- Consolidating all digital forensic resources into one location can provide a better collection of tools and require less duplication of hardware/software purchases.
- You have the improved ability to maintain a controlled environment when there is only one location these services are performed at, and digital evidence is maintained.
- A consolidation of employees with the same job functions allows these employees to use the institutional knowledge of one another to achieve their goals and does not limit their ability to collaborate amongst one another or to assist in troubleshooting the many challenges faced in digital forensics.
- Agencies can use the power of technology within the unit as a force multiplier instead of additional employees dispersed across your agency.
- New employees have more seasoned co-workers within their location to mentor and guide them as they learn the many digital forensic skillsets.

Disadvantages

- Employees needing any digital forensic service may need to travel a longer distance to obtain those services.
- Digital forensic employees must service the needs of all units within the agency and be aware of any specialized needs they may have.
- As your digital forensics department grows, you may become limited by the size of the office they are housed within.



Contemporary Personnel Considerations



[Image credit: spiceworks.com](http://spiceworks.com)

Dispersed Location

There are some agencies that can benefit from an organizationally dispersed model for their digital forensics needs. These agencies are usually large in geographical size, and/or have a very large volume of digital devices they must process. These agencies typically have larger and more well-established labs with the necessary staffing and tools. An additional approach when considering a dispersed model is to only disperse pieces of your digital forensic services such as the Internet Crime Against Children unit or your video recovery unit may be beneficial while still maintain a central location for all other services. There is a substantial cost investment in each tool needed in the collection and analysis of data from digital technology. When resources are unnecessarily dispersed, duplication of tools may be needed and will require addition financial investment by the agency.

Benefits

- Can provide services across a larger geographical area and may no longer require longer travel times for employees seeking the services of digital forensics.
- Allows for different locations for different types of services.
 - ⇒ For example, having employees who are assigned to the Internet Crime Against Children Unit work at an off-site location for safety and security purposes.
- Provides the ability for digital forensics teams to specialize in the investigations the detectives they are serving and the types of digital evidence needed to complete those investigations.

Disadvantages

- You will not have a “one-stop” shop for your digital forensic capabilities.
- There may be a substantial financial obligation to have multiple locations with duplicate hardware and software tools needed.
- There will be additional challenges to ensure all locations are conducting digital forensics in a forensically sound method and producing standardized products.
- Additional oversight may be required to ensure that proper training, software, and hardware is deployed across all locations within the agency.

Contemporary Personnel Considerations

Outsourcing to Private Vendors and Federal Counterparts

Developing, staffing, and maintaining digital forensics services in-house can take a significant amount of time and financial commitment. Many smaller law enforcement agencies operate some level of digital forensics service with only one or two employees dedicated to it. Agencies who are just beginning to deploy a digital forensics team or have very limited budgets/personnel can consider outsourcing some of their needs to their federal partners or private companies. By assessing the best approach to meet your agency's digital forensics needs, outsourcing some of your digital forensic services can improve your overall incident handling capabilities.

The United States Secret Service, among other federal and state agencies, offers many digital forensics services and training opportunities to local law enforcement. They have field offices around the country that your local agency can partner with to take advantage of their services. In addition, there are numerous private companies that offer specialized services such as chip-off, advanced electronic repairs, hard drive restoration/recovery.

Advantages

- Allows agency examiners to allocate their training and skills on core competencies needed to fulfill their department's needs.
- There is a reduced risk when outsourcing services not performed on a regular basis, such as chip-off, to a company that can produce more reliable results.
- It can offer cost advantages by not having to invest in the training and equipment when the service is not performed on a regular basis in-house.
- Service is provided without delay resulting in faster resolution.

Disadvantages

- Chain-of-custody records and reports may not conform with a department's standards.
- Vendors may need to be reimbursed to travel to local jurisdictions for expert witness testimony.
- Extra steps may need to be taken to protect the sensitive information contained on some digital devices.
- Physical evidence may need to leave the care and custody of the law enforcement agency - exposing it to the possibility of loss, theft or damage.

[Image credit: 911 Phone Repair](#)



DFU Synergy with Other Entities

Detective Lieutenant Devin Ross
Nassau County Police Department

In the world of cellular forensics, understanding the state of a mobile device is critical to an effective data extraction of your target device.

Because of this, it is crucial to consider the state of a device while planning an arrest, search warrant, or any other interaction with a subject when evidence being collected from their cell phone is going to be vital to your case. Before discussing tactics it is important to understand what these states are. A cell phone has two basic primary states which are before-first-unlock (BFU) and after-first-unlock (AFU). These states determine exactly what data is accessible in a locked "non-consent" phone and may be the difference in finding the critical piece of evidence that determines the outcome of a criminal case.

Before-first-unlock refers to the state of a device that has been powered off or restarted and has not yet been unlocked by the user. Both Apple iOS and Android devices utilize a file-based encryption system which means that the device needs to be unlocked with a password or pin after the phone turns on or reboots in order to access programs and data that are not essential to run the device. So basically, the files that you are able to get from a BFU extraction are the files the phone cannot encrypt because they are needed for basic functionality.

It can still be very useful to conduct a BFU extraction and you can find things such as, the date and time of last iCloud backup, and File Provider Storage (Dropbox, Google Drive and others). New research by the International Association of Computer Investigative Specialists have demonstrated that a significant amount of Snapchat data can be extracted in BFU mode including user account, uploads, logs, chats, contacts, images and videos.

You can usually get the iCloud account information from BFU extractions which would then allow an investigator to send Apple a warrant for the iCloud backup and in some cases get most of the same data that is available on the unlocked device.

After-first-unlock refers to the state of a device that has been unlocked at least once after being powered on or restarted. Since the encryption keys are now available in the phone, a lot more of the device data is accessible. These keys reside in the device memory until the phone is rebooted or powered off. It is generally agreed in the forensic world that an AFU extraction will provide you will approximately 95% of the user data and is the best alternative to having the device password.

AFU extractions while extremely comprehensive are still missing some data that you would expect to find in a "Full File system" extraction in an unlocked device. You will not get health data, native emails, cached locations, and significant locations. AFU extractions will also provide you will a higher level of detail about the device, accounts linked, and other data which again could be utilized to get additional warrants. There is technically one more device state which is unlocked and means the phone is open, the examiner has the password or it does not have a password. This device state obviously would provide the most comprehensive forensic extraction providing all the data that is contained in the device.

Understanding these device states is really just the beginning of the forensic process and as a law enforcement agency we have to adopt best practices to ensure we maintain an AFU device state if possible. This requires educating Patrol Officers, Special Operations, Crime Scene, Squad Detectives and any other units that may encounter a phone or a defendant with a phone.

Some considerations could be, for example, not letting a defendant turn his/her phone off prior to being arrested, or not allowing a defendant in custody to use their own phone to make phone call or send a text after which they turn the phone off. Even the basic tactic of removing a defendant's property from their person prior to police transport to ensure they can't hold a power button down handcuffed in the back of a police car is essential.



In some cases, we have to unlearn past historical practices.

In the past, serving a search warrant at a residence may have been the safest and tactfully sound way to go. In a case where the subjects cell phone is suspected to contain crucial evidence to that case, having that phone plugged in for 8 hours in the subjects end table means that phone is going to be in an AFU state which will yield very little to no evidence.

Lately my department, as well as many others, consider additional options during pre-operation meetings. In some cases especially conspiracy, or ICAC cases we have decided that the evidence is too valuable to allow the subject to lock that device.

Instead options like grabbing a subject on the street when they are getting out of their vehicle or walking out of a store is being used over an early morning search. In some cases we have waited for a subject to be actively talking on, texting, or surfing the web on their phone. This usually puts them in a distracted state. As they are being put into custody the phone is being removed and immediately turned over to the technical investigators.

While the basic tactics of securing a phone are the first step the device will still need to maintain power to remain in the AFU state. It should be noted that it is equally important to isolate the phone from the network to preserve the data from remote wipe.

In some cases, it may be possible to place a device in airplane mode or eject a sim card but the newer phones with ESIMS the only solution to properly preserve the device is a Faraday Bag (network isolation) with charger. It should be noted that since the phone is in a network isolation bag the battery will drain much more quickly than normal as the device struggles to connect to a cell tower.

The remote wipe functions are available in both Apple IOS and Android systems which means every single device recovered or seized needs immediate isolation and charge.



Again the tactics of not letting a defendant in custody use a phone until all the digital evidence is properly secured is crucial. For example, a defendant in custody could call a friend or family member from the designated prisoner phone and have that friend/family member send a remote wipe signal to wipe the device the next time it connects to the network. Understanding this process is very important for - you may want to make sure your phone evidence is secure.

After a device recovery, there are many additional logistic factors that must be addressed with the goal of preserving the phone data and maintaining AFU. The industry best practice is to get the digital device to the lab as quickly as possible or request technical service units respond to assist. There is no second chance with AFU mode and preparing arrest paperwork may take much longer than the phone will hold a charge. There are also legal considerations which need to be addressed for example it may take several days to secure a search warrant for the device and we don't want to lose the AFU status in the overlap. Again, reinforcing the best practice of getting the device to the lab as soon a possible.

The best way to mitigate these logistical hurdles and preserve as much digital evidence as possible is to have policies, procedures, equipment and education to guarantee success.

Detective Michelle Palamara
Buffalo Police Department

Ambiguous Precedent Case Law and Lack of Lawful Access Statutes

A leading theme related to regulatory considerations in policing, specifically within digital forensics, that can be found throughout case law and journal articles notes the following; pre-digital law cannot effectively be applied to the digital world.

Current case law regarding digital evidence is unclear and lacks specific guidelines involving lawful access. Most, if not all judicial jurisdictions are encountering legal concerns regarding the lawfulness of searches for digital evidence, and to what extent evidence can be admitted in court cases.

One of the most important cases that addressed the searching of cell phones is *Riley v. California* (2014). In *Riley*, the U.S. Supreme Court recognized that the ubiquity of cell phones, combined with their capacity to hold vast quantities of detailed personal information—potentially the “sum of an individual’s private life”—make cell phones so qualitatively and quantitatively different from people’s pre-digital property as to require a warrant to search one incident to an arrest.¹ *Riley v. California* did not further specify any standards that limit the scope of cell phone searches, and while examining current cases, courts across the country are taking different approaches.

While some courts have constrained police searches to certain types of data on the phone, specific time periods, or limited the use of the data, other courts have authorized warrants that allow the police to search the entire device.

In addition to requiring a search warrant to search a cell phone, *Carpenter v. United States* (2018)² ruled that a search warrant was required in order to obtain cell-site location information (CLSI). While it was acknowledged that the government is able to access CLSI data under other circumstances without a warrant such as the Stored Communication Act or exigent circumstances; in order to use the data acquired against an individual criminally it must be obtained by having probable cause and a search warrant.

The Abandonment Doctrine authorizes the searching and seizure of abandoned property. However, the ninth circuit contends abandonment of digital device does not expressly mean abandonment of the data it contains. An example currently being argued is *U.S. v. Hunt* (2024)³. The Court should clarify if the “abandonment doctrine” does not apply to data stored on cell phones – specifically if there is still an expectation of privacy for the data stored on the device even if the owner lost control of the device itself.



Legal & Regulatory Considerations

The issue of abandonment continues to require additional legal clarification when it comes to digital evidence such as cellular devices or smart phones.

If an individual has data that is stored on a cloud server, and they are able to access it from a device other than the one that was abandoned, they still have a possessory interest and control over said data. Moreover, if an individual can control the data on a device remotely, which is common for many smart phones, then they may argue that the data wasn't abandoned. Ultimately, the most legally defensible way to proceed is to obtain a search warrant versus relying on the Abandonment Doctrine.

Additional legal challenges arise from limits imposed on the scope of a search warrant. It has already been stated that cell phones hold a tremendous amount of personal data, and courts have ruled that its rare that one can demonstrate suitable probable cause that would convince a judge to authorize a complete search of a phone *Richardson v. State of Maryland Court of Appeals (2022)*⁴. *Commonwealth v. Jones (2018)*⁵ addresses legal issues with compelling a defendant to give their passcode. In this instance the court has to prove that the defendant knows the passcode. However, the Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." Similarly, art. 12 provides that "[n]o subject shall . . . be compelled to accuse, or furnish evidence against himself."

The above referenced court case demonstrates the changing nature of legal interpretations and the lack of clear governance authorizing or limiting law enforcement. With 6.4 billion smartphone users worldwide, 96% of adults between the ages of 18-29 own a smart phone, and 74% of Americans say they would not leave their cell phone at home (PewResearch.org). Phones play an important role in our daily lives which is why phones so frequently hold evidence of crimes. It is increasingly necessary to establish proper and legal guidelines when it comes to how and what law enforcement can access.



The 4th Amendment of the United States Constitution prohibits unreasonable search and seizures and sets requirements for issuing warrants.

"The right of the people to be secure in their persons, houses, and papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or Affirmation, and particularly describing the place to be searched, and the persons or things to be seized."



Legal & Regulatory Considerations

Sergeant Richard Geiger
Metropolitan Police Department (Washington DC)

Introduction

Mobile phone ownership in 2024 transcends age, gender, race, socio-economic status, and practically every other identifiable category that an individual can fall within. According to the Pew Research Center, 97% of Americans own a cellphone, 90% of which are smartphones. Those numbers represent a 16 and 55-percent increase, respectively, from mobile and smart phone ownership from 2011¹. This upward trend of cellphone ownership isn't unique to the United States however, at least fifty-eight countries have over 100 cellphones per 100 of its citizens². As cellphone ownership has increased, so too has law enforcement's reliance on the contents found within them to bolster criminal investigations. The result of this reliance led to a flurry of Fourth Amendment challenges to cell phone searches, culminating with the Supreme Court's clear command that search warrants are generally required to conduct a search of a cellphone³. Less clear, however, is to whether there are any limitations on the type of data or the timeframe of data that can be seized pursuant to a search warrant. This section seeks to lay out the legal landscape across MCCA jurisdictions and across the federal district courts and courts of appeals.

The Legal Landscape

We analyzed legal precedents set by courts and laws passed by legislatures across the country to determine how they have affected the way in which law enforcement obtains data from devices in criminal investigations. In the context of temporal or file-type limitations, the Honorable Robert Lasnik of the United States District Court for the Western District of Washington opined that "[t]he state of the law is admittedly opaque"⁴. Unlike other types of Fourth Amendment cases such as vehicle searches⁵, searches incident to arrest⁶, and even searches of phones⁷, courts have been reluctant or unable to articulate a bright-line rule, applicable across the board, in determining the appropriateness of a time or file-type limitation when seeking judicial authorization to conduct a search of a cellphone.

A. THE FACT-SPECIFIC NATURE OF TEMPORAL OR FILE-TYPE RESTRICTION INQUIRIES

Our research revealed a possible reason for the lack of clarity on this topic: each of the legal decisions that upheld or suppressed search warrants that were alleged to be overbroad or unparticular engaged in a factual discussion that played a significant role in the ultimate decision. The fact-specific discussion in these decisions have primarily touched upon the following contours of the warrant:

1. The affiant's training and experience. The affiant's training experience, including facts and reasonable inferences drawn from those facts and experience, and how that factors in to the affiant's knowledge of the type of data and/or the timeframe of data that he or she seeks to seize from the device can help provide basis for a broader (or limitless) search.
2. The type of offense that law enforcement is investigating. Specifically, "broader searches may be permitted where there is probable cause to believe that a narrower search will miss hidden or mislabeled evidence"⁸. The Maryland Supreme Court in Richardson cites with great deference an article by Adam M. Gershowitz⁹ suggesting that the type of crime (i.e. child pornography, financial crimes) may influence whether a broad search can be conducted.

Following that same logic, street crimes, such as drug distribution, or offenses involving co-conspirators may also be a factor in determining the appropriateness of the scope (temporal and file-type), or if a narrowing scope is even required.



Legal & Regulatory Considerations

3. The nexus between a suspect to a digital device. While the above section mentions that the type of crime is important in the calculus to determine temporal or file-type limits, courts have also factored the suspect's actual or inferred use of a device relative to their criminal activity. For instance, then-Chief Judge Beryl Howell of the United States District Court for the District of Columbia upheld the search of the devices – and did so without limit - in part because the victim “knew that [the suspect] had used the phone to engage in the relevant offense”¹⁰. Similarly, the United States Court of Appeals for the Fifth Circuit, sitting en banc and without explicitly deciding the question of temporal or file-type scope, recognized that multiple phones in a car with narcotics can indicate criminal activity.¹¹ The presence of an actual or inferred nexus between a suspect and the use of digital devices is akin to a threshold question that, when answered in the government's favor, then allows courts, such as the District Court in the District of Columbia and the en banc Fifth Circuit, to analyze whether a temporal or file-type limitation is necessary or not (or, at minimum, whether the good-faith exception applies).

4. The inclusion and exclusion of facts and conclusory statements. Several courts have gone into a great amount of discussion on the premise that the warrants subject to review were “bare bones,” or those failing to “state more than ‘suspicions, or conclusions without providing some underlying factual circumstances regarding veracity, reliability, and basis of knowledge’”.¹² While the overwhelming majority of those courts have subsequently determined that data seized from the devices was admissible under the good-faith exception doctrine, several courts have invalidated the warrants based on the inability to curtail a broad sweep “in describing the items subject to seizure” that was based on nothing but “conjecture” and “belief”¹³. This reasoning is similarly applicable to temporal restrictions. In both *Schubert* and *Burns*, the highest courts in the State of Ohio and the District of Columbia, respectively, not only invalidated the warrants, but refused to extend the good-faith doctrine (which will be discussed in greater detail below) to the searches.

B. GOOD-FAITH EXCEPTION IN TEMPORAL & FILE-TYPE RESTRICTION CASES

United States v. Leon is the seminal Supreme Court case dealing with the good-faith exception to the Fourth Amendment. *Leon* has had arguably the most significant impact on legal challenges relating to temporal and file-type restrictions. Courts analyzing these types of challenges have oftentimes discussed the good-faith exception's applicability, and have ruled generally in three different ways. First, several courts have specifically declined to rule definitively on the question of scope, instead resolving the case by applying the good-faith exception and knocking down the suppression challenge.¹⁴

Second, several courts have ruled that while the warrants were overbroad in terms of timeframe and/or file-type, the admission of electronic data was not suppressed due to the officers' good-faith reliance on the warrants that authorized the searches.¹⁵

And in several instances that should caution law enforcement when using “catchall” language, several courts have ruled that not only were the search warrants to conduct an extraction of digital devices overbroad in terms of time or file-type limit, but that law enforcement did not act in a good-faith basis in relying on them, thereby suppressing the data (and, arguably worse, subjecting the affiant to reputational harm)¹⁶.

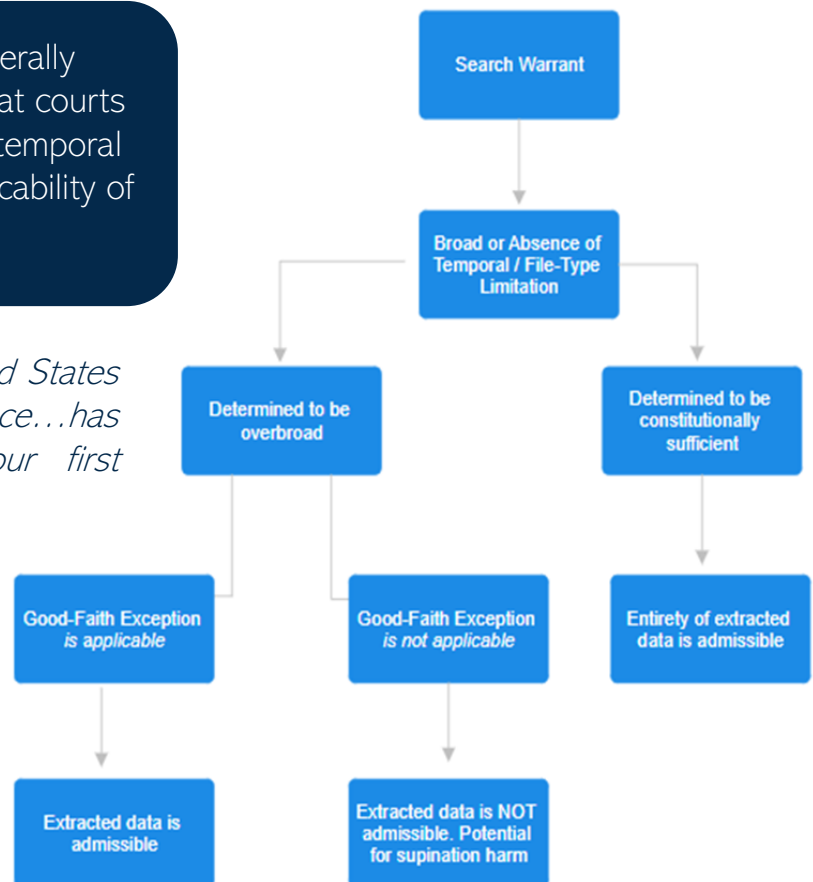


Legal & Regulatory Considerations

To the right is a diagram that generally summarizes the analytical process that courts have undertaken in their analysis of temporal and file-type restrictions and the applicability of the good faith doctrine:

Though the Supreme Court of the United States opined that “suppression of evidence...has always been our last resort, not our first impulse”¹⁷,

...the Burns and Schubert courts have shown that full – versus piecemeal¹⁸ – suppression of evidence and an outright rejection of the good faith argument is a reality and something that law enforcement must confront. Law enforcement, as a result, should be hesitant to rely on the good-faith exception when preparing warrants that might be deemed overbroad or lacking particularity.



C. RESTRICTIONS PLACED UPON MCCA-PARTICIPATING AGENCIES

The cases cited thus far have provided some guidance on how law enforcement is to navigate the ever-evolving field of digital device searches. We sought to assess the real-world impact of case law or legislative action that has largely curtailed law enforcement’s ability to search for and seize “any and all information and/or data” from a digital device¹⁹. Specifically, the MCCA Digital Evidence group were asked whether their digital evidence labs or processing centers receive search warrants with limiting language, either by timeframe or by file-type, similar to those discussed in the previous sections.

Law enforcement in Buffalo (NY), Las Vegas (NV), Oklahoma City (OK), Tulsa (OK), Raleigh (NC), and San Diego (CA) indicated that the warrants they receive for digital extractions are not limited temporally or by category of data. Similarly, we identified several court cases that have held that a warrant is sufficiently particular if its scope is limited to evidence of a particular crime. Put another way, these cases outline the proposition that bar of constitutional particularity required by the Fourth Amendment is met when an officer “stat[es] what crime is under investigation.”²⁰



Legal & Regulatory Considerations

The legal landscape for the rest of the MCCA Digital Evidence group, however, is much different. Law enforcement in Washington (DC), Prince George's County (MD), Denver (CO), Fairfax County (VA) and, Mesa (AZ), as well as law enforcement in Canada (Toronto, Vancouver, and Peel, all indicated that they generally receive requests for digital extractions pursuant to a search warrant that are limited temporally and/or by file-type. These types of restrictions are likely the result of temporal and file-type restriction challenges percolating through the various court systems on a state and federal level, such as the Burns decision in Washington DC and the Richardson decision in Prince George's County (MD). These restrictions present difficulties to law enforcement seeking the warrants, as well as the examiners tasked with extracting and oftentimes deciphering the data to ensure compliance with the search warrant.

Law enforcement in Los Angeles (CA), meanwhile, indicated that the warrants they receive for digital extraction are limited not necessarily by court precedent, but rather through the legislative enactment of the California Electronic Communications Privacy Act ("CALEPCA"). CALEPCA is one of, if not the only, pieces of state or federal legislation to directly address temporal or file-type restrictions in the context of searches of electronic data. While exceptions to the temporal or file-type restriction are codified in CALEPCA, Section 1546.1(d)(1) articulates that, generally, warrants shall describe with particularity the information to be seized by specifying, as appropriate and reasonable, the time periods covered, the target individuals or accounts, the applications or services covered, and the types of information sought.

D. GUIDING PRINCIPLES

There is a lack of a clear consensus regarding temporal or file-type restrictions. This gap may create unintended and deleterious consequences impacting law enforcement's capacity to conduct legal searches of digital devices. Probable cause determinations "are fluid concepts," "not readily, or even usefully, reduced to a neat set of legal rules"²¹ and a "one-size fits all" set of rules would likely not account for the evolution of digital devices as well as the technology used to lawfully access the data within them.



Legal & Regulatory Considerations

It is difficult for law enforcement to know with any reasonable degree of certainty precisely where on the phone evidence of the crime is being secreted, and just how long planning, searching, or discussing the crime has been ongoing. Some options are offered for consideration to mitigate these uncertainties:

- 1) Law enforcement conducting a lawful search of a device based on temporal or file-type restrictions should, consider preparing follow-up search warrants as necessary to expand the scope of the first warrant.
- 2) Law enforcement should leverage current technology, like Cellebrite or GrayKey, to generate data reports that comport with temporal or file-type restrictions placed upon law enforcement acting pursuant to the search warrant. In the absence of the ability to do so, law enforcement should seek input from actors like Cellebrite or GrayKey on how best to cabin the search authorized by the search warrant.
- 3) Those authoring search warrants for the seizure of digital data may be able to obviate the need for temporal or file-type restrictions, or at minimum be able to expand the scope beyond what was initially possible. Law enforcement should describe in great detail the process by which a filter team or a wholly uninvolved investigator would receive the full extraction, with no temporal or file-type restriction, or parsed data. ONLY the data that the filter team determines to be evidence of the crime being investigated should only be provided to the assigned investigator.



CONCLUSION

The complexities of searches of digital devices render the current state of temporal and file-type restrictions confusing. Law enforcement is best served taking a cautious approach to search warrant writing and execution in the digital evidence sphere. The impact that lawfully obtained digital data can have on the successful prosecution of our most important cases cannot be understated. As technology continues to evolve, so too must law enforcement.



Digital Evidence Management

Sergeant Bryan Wang
Digital Forensics Lab
Arlington Police Department

Impact on Police Investigations

Digital Evidence Management (DEM) is the process used by law enforcement agencies to collect, preserve, analyze, and present digital evidence. This evidence is collected from a range of sources, such as computers, smartphones, and surveillance systems. Over the years, DEM has significantly evolved with modern day technology, making police investigations more efficient and effective.

The development of new technology and digital tools has transformed how evidence is gathered and maintained. Forensics software enables investigators to acquire digital evidence and confirm that the original data that was acquired has not been altered. Techniques like imaging hard drives and securing digital files ensure that evidence remains intact and admissible in court. Digital forensics tools offer analytical capabilities that allow investigators to examine large amounts of data quickly. This examination of data helps uncover critical information, such as, communications, location data, and digital footprints. This enables investigators to identify suspects, track activity, and establish any connections in the case.

Digital evidence management systems centralize and organize digital evidence in secure, searchable databases. These systems offer features like digital chain-of-custody tracking, automated evidence tagging, and detailed audit trails. This approach reduces the risk of evidence tampering or loss and improves the efficiency of evidence handling and retrieval. This also provides a level of data stewardship, which ensures the data collected is accessible, usable, safe, and trusted.

Collection and Data Stewardship

While different states and local municipalities vary in laws and regulations, agencies must consider how to obtain and maintain the data that is collected. As with all evidence, agencies must maintain a strict chain of custody to ensure that evidence is not tampered with or compromised. This involves detailed documentation of who handled the evidence and when. Law enforcement is often required to acquire a warrant to collect digital evidence. This evidence must be collected in a manner that makes it admissible in court. This involves adhering to specific rules and standards, such as ensuring that evidence is not collected through illegal searches or seizures. Ultimately the primary purpose is to gather evidence that can be used to prosecute criminal activity, which is why it is important to have policies in place with specific requirements related to data collection.

In addition to the practices of data collection mentioned, it is important to consider security for the collected data. Data security focuses on protecting digital evidence from unauthorized access, tampering, loss, or destruction.

Policy Considerations

Access Control: Strict access control to ensure only authorized personnel can access the digital evidence.

Encryption: Ensures that data cannot be read or altered without appropriate decryption keys.

Secure Storage: Digital evidence must be stored in secured environments, such as isolated and controlled forensics labs with restricted access. Any digital storage should have the ability to log and monitor all actions taken with the evidence.

Incident Response: In the event of a security breach or suspected tampering, a well-defined incident response plan should be in place. This plan should include procedures for investigating the breach, mitigating damage, and restoration of any lost data.



Captain Dana V. Ferreira
Police Liaison Commander
Fairfax County Police Department

One of the most challenging aspects of deploying an effective digital forensics strategy is obtaining the necessary tools, equipment, and training to be successful. Implementing various solutions and technologies may require significant funds, to cover both initial outlays for equipment and recurring costs for services and software. Agencies need to consider balancing budget-minded options while also ensuring that investments can continue to serve them as needs evolve. However an agency chooses to proceed, establishing a roadmap for deployment and operations can help keep costs predictable and within budget.

Training

A foundational component of a digital forensics strategy is the training of qualified staff. Training can be obtained through various means, and costs vary based on the nature of the coursework. Some vendors include training with subscriptions for a specific service or software, while others offer training and certification on their products at an additional cost. Another option may be training for law enforcement through non-governmental organizations, private-government partnerships, and federal task force membership, offered at reduced rate or, in some instances, for free.

It is important that, as part of an implementation plan, leadership determines the level of certification they wish their examiners to obtain. Ultimately, associated costs will depend heavily on this factor. Agencies can sometimes mitigate these costs by volunteering to host vendor trainings at their facilities or recruiting additional attendees.

Additionally, there are commercial training packages where examiners can attend an unlimited amount of courses during a specified time period (normally a year) for a fixed price. As the digital forensics field is constantly evolving with the ever-changing consumer electronics market, examiners will need to attend continuing education offerings throughout their career.



Software

Software used in various digital forensic processes—from unlocking and decrypting data to analyzing findings—typically comes with two pricing models: perpetual licenses (where software is purchased and can be used in perpetuity, but access to updates and support may require a renewal) and subscription services (access to a license is purchased and the software can only be used while there is an active subscription). The trend in the industry is toward the subscription model. Accordingly, agencies need to be prepared to allocate funds on a recurring basis toward a specific software solution, and to budget for increases in subscription costs at renewal.

These cost increases can be forecasted, and mitigated to a degree, by establishing multi-year contracts with software providers. For example, determining a pre-selected schedule for cost increases allows an agency to anticipate these costs over the life of the contract. It also ensures that cost increases are predictable, and at a level amenable to both the vendor and the agency. Multi-year contracts can also ensure continuity of services, so software does not become unavailable to examiners while an agency and the vendor negotiate pricing at the conclusion of a subscription period.

A more recent trend in the digital forensics field, and an important consideration prior to investing in equipment, is the concept of “Software as a Service,” or SaaS. The SaaS model effectively takes the requirement to procure and maintain infrastructure out of the hands of the customer, and instead places it with the software vendor or a third party. Leveraging cloud computing—where processing is handled on shared resources in decentralized data centers—SaaS allows technical staff to focus on the digital forensic process without the need to maintain as much physical equipment (computers, servers, etc.). SaaS does come at a higher cost than traditional software that is managed by the end-user. However, agencies may find that this cost is offset by the fact that they do not need to supply as much technical staff, physical infrastructure, or data backup services.

When procuring software, an agency should look at the number of anticipated investigations they will conduct to determine the proper scale of solution required. For example, a smaller agency that anticipates examining a dozen phones in a calendar year would not be well served by many of the premium-tiered (and priced) unlimited services offered by various vendors. Recognizing this, many software solutions include per-action pricing, or the ability to purchase a package with a certain number of allowed uses with the option to obtain more if needed.

Equipment

Examiners require a variety of specialized equipment to complete the forensic process from device collection through prosecution. While some of these tools are required whether the agency opts to host their solutions on site or utilize SaaS (such as Faraday bags and boxes, repair kits, various power sources, etc.), others can be scaled based on need. For example, if an agency is using cloud-based resources for analysis of data, they may not need to procure workstations with as much power as one who is hosting their solutions on-site. Once a digital forensics team decides which type of software they will use and select a vendor, they should coordinate with that vendor to determine the optimal specifications for the chosen solution. Ensuring that equipment will not just meet the needs of today, but also the needs of the future, can help reduce the need for repeated and costly upgrades.



Conclusion

The costs associated with running a successful digital forensics unit can be daunting and do not always correspond to the size of the team and number of devices processed. Some departments may consider partnering with other similarly-situated agencies to mitigate costs and share resources. This can help defray costs of licenses, capital equipment, and training, and ensure access to quality equipment and skilled investigators for criminal investigations. Whether an agency chooses to form a multi-jurisdictional team or create their own digital forensics unit, it should consider the level of training desired, the scope and volume of anticipated investigations, and the long-term plan for the team. Evaluating these factors prior to embarking on this journey can assist with determining an appropriate budget and ensuring that costs are predictable and reasonable.



Addressing Privacy and Civil Liberty Concerns

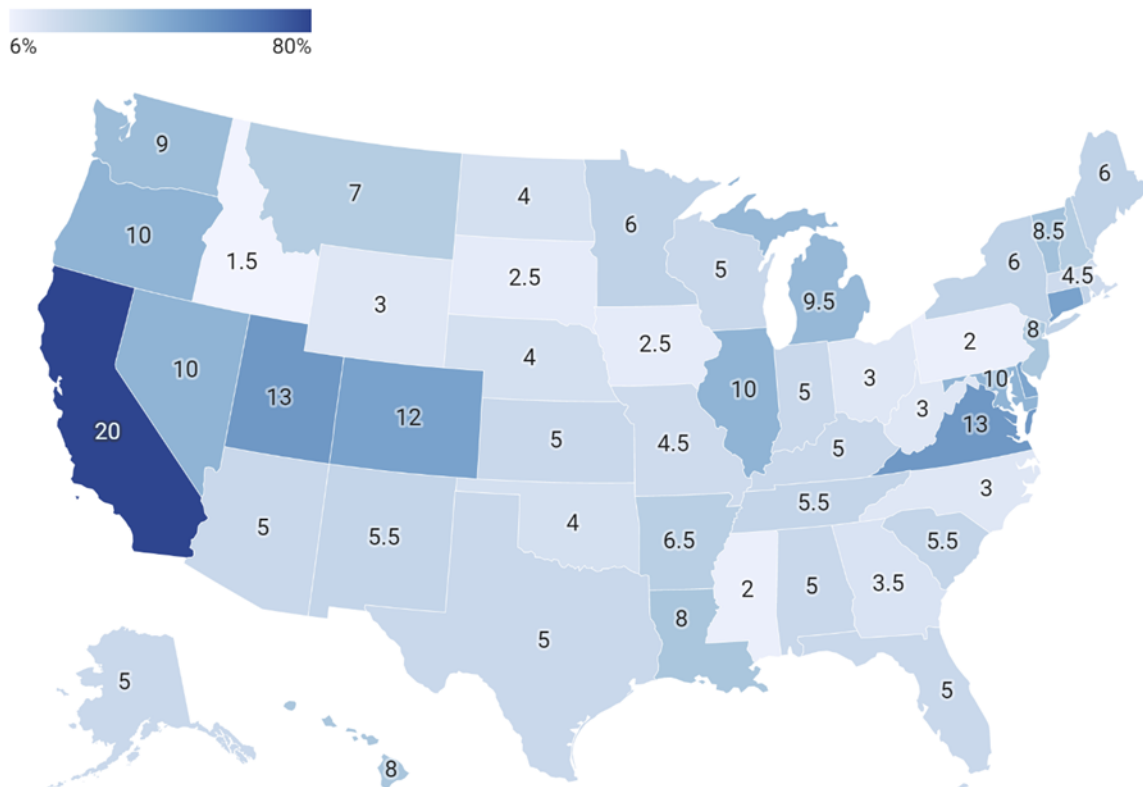
Lisa Merzwski
Supervising Criminalist
San Diego Police Department Crime Laboratory

The federal government enacted the Electronic Communications Privacy Act (ECPA) in 1986. This statute protects wire, oral, and electronic communications including the data stored electronically. States such as California have gone beyond this federal statute enacting their own ECPA laws that regulate collection, use, and disclosure of electronic communication and location information by law enforcement agencies. It requires a warrant before law enforcement can seize the contents or metadata of communications, demand location records from cell phone providers, or use a StingRay to gather information about smartphones. The ECPA in California also specifies that only the primary user can give permission to access a digital device, not necessarily the person who paid for the device and service.

Obtaining a warrant for law enforcement agencies is nothing new. However, the sheer amount of digital data in modern criminal cases requires navigating the complex issue of privacy laws. Extracting a mobile device is an all or nothing endeavor. The tools cannot generally pick and choose which data to extract. Therefore, a warrant may limit the data that can be analyzed and by whom and for how long. Also, law enforcement agencies must then protect this data and prevent outside persons from accessing it.

Privacy by state scores - 2023

Each state was scored out of 25 and given a percentage value based on this score.



Source: [A state-by-state evaluation of internet privacy laws - DCN \(digitalcontentnext.org\)](https://www.digitalcontentnext.org/)

Addressing Privacy and Civil Liberty Concerns



Image of San Diego, CA

In San Diego, California the City Council passed an ordinance known as the [Transparent and Responsible Use of Surveillance Technology \(SDMC 210.0103\(b\)\(2\)\)](#). The Surveillance Ordinance requires that for each technology that meets the criteria for surveillance, City Departments must:

- Hold at least one or more community meetings in each City Council district where the proposed surveillance technology is deployed, with an opportunity for public comment and written response.
- Prepare a Surveillance Use Policy that includes the purpose, use, data collection, data access, data protection, data retention, public access, third-party data sharing, training, auditing, oversight, and maintenance.
- Prepare a Surveillance Impact Report including description, purpose, location, impact assessment, mitigations, data types and sources, data security, fiscal cost, third-party dependence, alternatives, track record, public engagement, and comments.
- Present the item to the Privacy Advisory Board for review.
- Present the item to City Council for the acquisition and deployment of all new and currently used surveillance technologies.
- Provide annual reports on surveillance technology use, impact, and acquisitions.

While the technical definition of surveillance is monitoring activities, this ordinance is very broad and impacts many departments. Technologies that fall under the ordinance include Drones, License Plate Readers, Helicopters, Smart Street Lights, Body worn cameras, DNA databases, and Digital Evidence extraction and analysis tools to name a few.

This process has taken hundreds of man hours and is currently ongoing. The San Diego Police Department (SDPD) had to have very clear procedures in place for each technology. Below is an excerpt of how the SDPD addressed the use of digital evidence analysis tools.

Digital evidence captured from the public during an investigation either through proper legal (search warrant) or consent-based authorization, can provide crucial insights into the nature of the crime being investigated. Finding a way to capture vital clues and/or evidence rapidly and in a forensically sound manner is of utmost importance. SDPD has used a software solution countless times to help victims of serious crimes including homicides and violent sexual assaults.

Addressing Privacy and Civil Liberty Concerns



The digital software tool proposal from the Department safeguards civil liberties. It is only utilized when prior proper legal authority (search warrant) was granted or with written consent of the device owner/user. The software is only used within the SDPD building on configured computers by approved individuals and is controlled by the department. Because the technology is only used when proper legal authority (search warrant) or with the written consent of the owner/user was obtained during extraction, there are no Fourth Amendment implications.

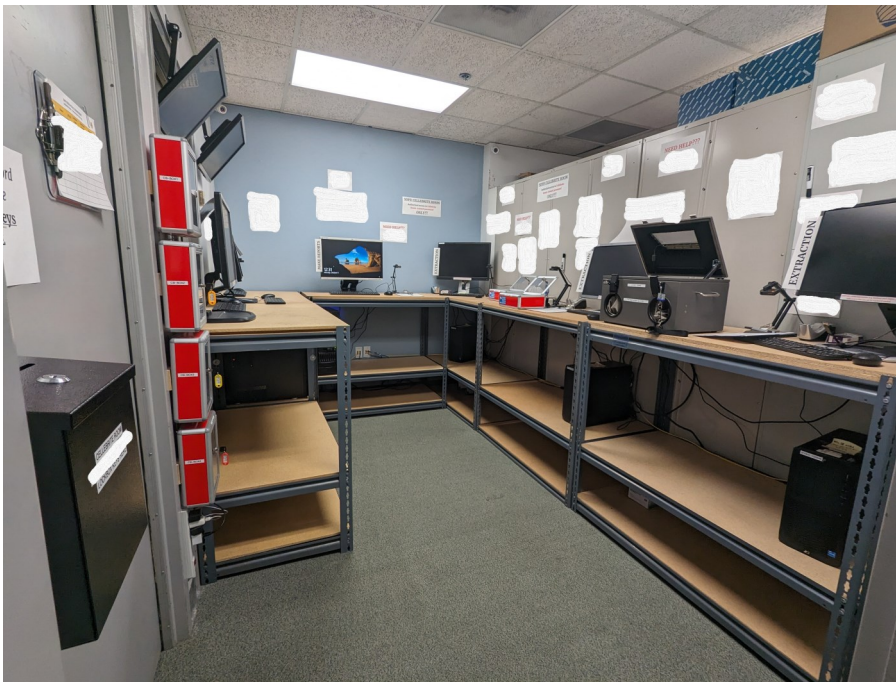
No alternative with a lesser economic cost or impact on civil rights or liberties would be as effective. The department utilizes the top digital forensic tools on the market today. Each tool's proprietary software is capable of slightly different extractions. Using all tools available to the department ensures investigators are provided the best data for their investigations. The cost to the department of the loss of this software would mean no data would be provided in many criminal investigations. This would be at great cost to public safety and the prosecution of serious crimes.

This software is used on secure computer systems that are not connected to the department network or have Internet access. There is no public access to the data analyzed by the software. If a criminal defendant wishes to obtain the interpreted data from the software as it relates to their case, it must be obtained through a court order or the discovery process.

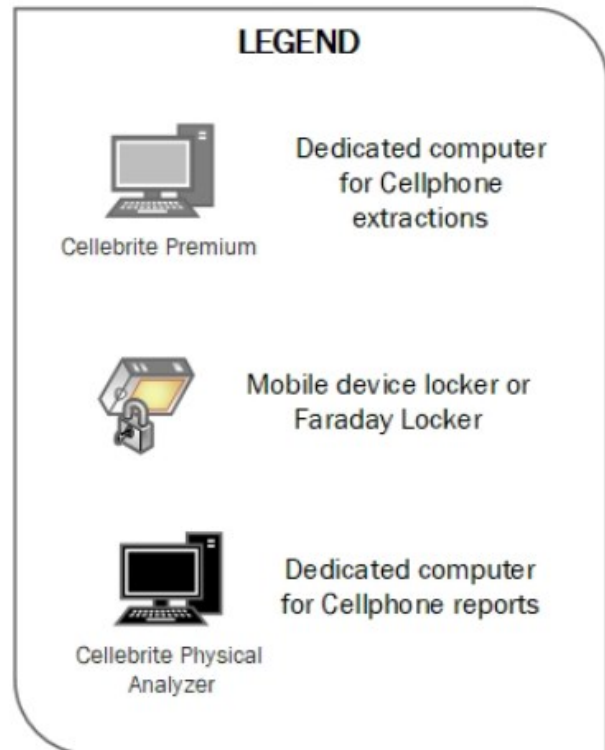
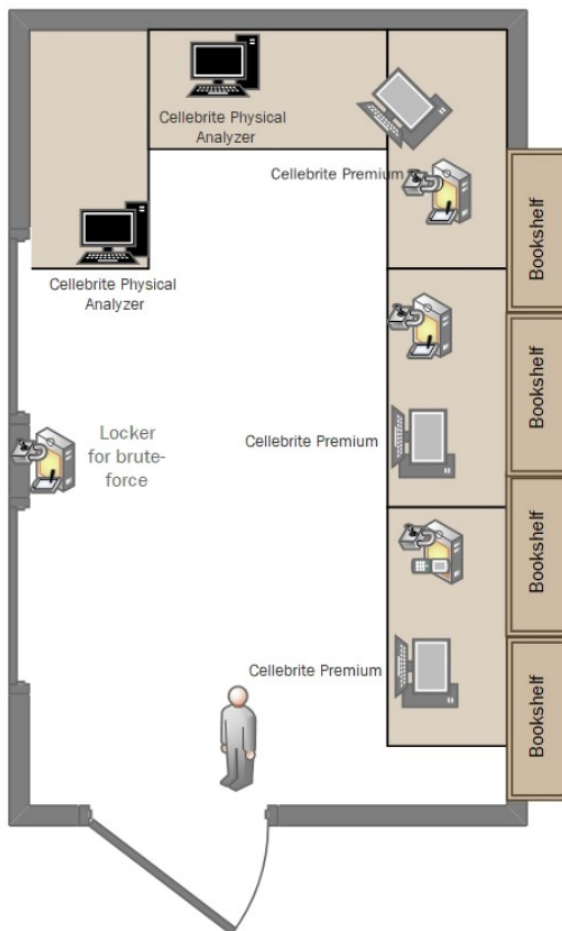
The SDPD received approval to use digital evidence extraction and analysis tools per the use policy presented to City Council. Addressing privacy and civil liberty concerns should not prevent the use of these valuable tools. Protecting the data is very important. However, protecting a law enforcement agency's network from this data is also important. These devices can have malicious software that can cripple a network. These rules, regulations, and laws will vary by Country, State, City, and location.

Example: Faraday Room

Images courtesy of the San Diego Police Department Crime Laboratory



The San Diego Police Department created this heavily monitored, key card accessed cell phone extraction room with Cellebrite Premium extraction computers and report making computers that can be accessed 24/7 by trained investigators. It is equipped with faraday boxes and brute force lockers. This is essentially a digital property room that also stores the data and reports on a NAS once the investigator is finished with the phone. This allows investigators from all over the city to extract phones on an as needed basis without making an appointment with the laboratory.



[Link: San Diego Police Department Crime Laboratory Forensic Technology Unit Manual](#)

The Impact of A.I. on Digital Forensics

Christian Quinn

Managing Principal, Fulcrum Innovation LLC

Technology will not replace trained professionals; however, it will help good people do their best work. Artificial Intelligence (AI) has the potential to revolutionize the field of digital forensics, offering significant benefits while also presenting notable challenges. It is crucial to consider both its potential and the hurdles that must be overcome to harness AI's benefits. This section aims to offer an overview of the transformative impact AI is already having on digital forensics, and the utility that practitioners hope it brings.

Potential Benefits of AI in Digital Investigations

- 1) **Enhanced Timeline Analysis** | One of the most promising applications of AI in digital forensics is in timeline analysis. The volume of data generated by digital devices, including location and health data, can be overwhelming and difficult to analyze. AI algorithms can sift through vast amounts of information to identify patterns and anomalies, helping investigators pinpoint critical events within specific time frames. This capability not only streamlines the investigative process but also ensures that critical insights are not overlooked.
- 2) **Automating Data Summarization and Reporting** | AI-powered tools have the potential to automate the summarization of findings, making it easier for investigators to generate comprehensive reports. These tools can highlight key pieces of evidence, organize data logically, and present it in a format that is accessible to non-digital forensic unit investigators. By simplifying the interpretation of complex data, AI can enhance collaboration and understanding among various stakeholders involved in an investigation.
- 3) **Streamlining Back-End Processes** | The integration of AI into case management and workflow systems can significantly enhance the efficiency of back-end processes. AI can automate routine tasks, manage workflows, and ensure that cases are handled promptly and systematically. This not only reduces administrative burdens, it allows investigators to focus more on critical aspects of their work, and ensures "time-to-justice" that adheres to appropriate judicial standards.
- 4) **Machine Learning in Evidence Prioritization** | Agencies like the Tulsa Police Department are already leveraging machine learning tools to expedite the triage process. While these tools may not always locate specific pieces of evidence, they are effective at identifying folders and areas of interest, thereby reducing the time required for initial evidence assessment. This accelerates the overall investigative process and allows for quicker decision-making.
- 5) **De-Aging Software in Undercover Operations** | AI-enabled de-aging software is being utilized in undercover operations to alter the appearance of agents, enhancing their ability to infiltrate groups engaged in human trafficking and the distribution of child sex abuse material. This application demonstrates AI's versatility and its potential to augment various facets of investigations beyond just digital forensics.
- 6) **Object Recognition** | Object recognition is being explored to identify and categorize items within digital images and videos. This technology can be particularly useful in cases involving large volumes of multimedia data, where manual analysis would be time-consuming and prone to human error.



The Impact of A.I. on Digital Forensics

Challenges and Concerns

1) **The Threat of Deepfakes** | One of the most significant concerns regarding AI in digital forensics is the rise of deepfakes. These synthetic media, which can convincingly alter audio and visual content, may call into question the authenticity of digital evidence. While the technical manipulation of media is a challenge, the perception problem it creates among jurors and the public is even more concerning. Ensuring the authenticity of digital evidence is paramount, and AI tools must be developed to detect and mitigate the impact of deepfakes and synthetic media effectively.

2) **Data Replication and Authentication** | The replicability of AI findings and the proper authentication of AI-generated evidence pose potential challenges. For AI tools to be widely accepted in forensic investigations, they must produce consistent and verifiable results. This necessitates rigorous validation processes and standardized protocols to ensure that evidence where AI comes into play still meets judicial standards.

3) **Ethical and Privacy Considerations** | The use of AI in digital forensics also raises ethical and privacy concerns. The collection and analysis of vast amounts of personal data must be conducted in a manner that safeguards individual privacy rights. Additionally, the potential for AI to be used in ways that could infringe upon civil liberties must be carefully monitored and regulated.

Future Opportunities and Considerations

1) **Custom Large Language Models (LLMs)** | Some agencies are experimenting with custom LLMs to enhance their investigative capabilities. These models can be tailored to specific forensic needs, providing more accurate and relevant insights. However, the development and deployment of these models require significant expertise and resources.

2) **AI in Interview Synopsis Processing** | There is growing interest in using AI to process interview synopses. While the current state of the technology may not be fully reliable, ongoing advancements hold promise for improving the accuracy and efficiency of this application. Continued research and development are essential to realize the full potential of AI in this area.



Conclusion

The agencies not yet leveraging AI acknowledge that there is a need to be more informed of its potential. As awareness grows, more agencies are likely to adopt AI tools, driving further innovation in the field of digital forensics. As emergent technology continues to evolve, it is imperative for police executives to stay informed about the latest advancements in AI, and to foster a culture of continuous learning within their agencies. By embracing AI and addressing its challenges proactively, law enforcement can leverage this powerful technology to enhance public safety in an increasingly digital world.



Buffalo Police Department, Buffalo New York

Including digital forensics as an investigative tool has become the norm for Buffalo Police Detectives, especially the Homicide Unit. In June 2022 Homicide detectives were called in for a single gunshot wound to the head where the victim did later succumb to his injury. After a thorough investigation, the detective realized there was little in terms of physical evidence and he turned to the Digital Forensic Unit.

Detectives determined the vehicle that the suspect was believed to have been shot inside was supported through vehicle forensics. Detectives were able to conduct forensic exams of two mobile devices and the vehicle, further shaping the direction of the investigation. The departments forensic examiner, using the data from two cell phone extractions and the vehicle infotainment system, was able to narrow down details of the crime leading up to and following his death; further narrowing the window of his murder down to mere minutes. Subsequent to the indictment and arrest of the suspect, the district attorney's office worked closely with homicide detectives and the forensic examiner to prepare this case, built on digital forensic evidence, as it went to trial in May 2024. After hours of expert testimony, thorough explanation of the tools used and the data obtained, the jury rendered a guilty verdict and the suspect was sentenced to 35 years.



San Diego Police Department Crime Laboratory

4 Year Old Brute-Force Case

At the time, one of the oldest cell phone brute-force cases in Southern California – San Diego County was instrumental in solving a SDPD Homicide case. The case involved a SDPD Homicide that implicated at least two suspects. This was considered one of San Diego County's oldest GrayKey cases.

Originally, the cell phone was submitted to the Chula Vista Police Department (one of the 1st agencies in southern California to purchase the GrayKey tool). The phone was subsequently transferred to the SDPD Crime Laboratory for its final destination and to continue the brute-force process. For 4 years, 4 months, and 29 days this cell phone was charging and going through multiple codes. It wasn't until February 24, 2023 that the cellphone finally unlocked. The laboratory was informed by the Deputy District Attorney Investigator that the case resulted in a hung jury in December 2022 and the DA's office was re-trying the case in 2023. The DA's office was considering an attempt by another agency to possibly try a different method for an unlock.



The data from the unlocked cell phone was extracted and reports generated for an immediate review by investigators. We were later informed by investigators that the data from that cell phone was critical, and that relevant location data was used in court. The location data placed the cell phone near / at the scene of the crime. Additional data from this iPhone also provided helpful information to strengthen the case against the defendants. If this case in December 2022 did not result in a hung jury, the cell phone would not have unlocked in time to present valuable data for the courts.

San Diego Police Department Crime Laboratory

2023 San Diego Library Shooting

In May of 2023, a shooting occurred at a library in downtown San Diego resulting in a homicide. At the time, it was not known whether it was an isolated incident or an active shooter scenario. There was video footage of the suspect fleeing the scene, but the suspect was unidentified. Using cell phone data, detectives were able to find the suspect, their co-conspirator, and the murder weapon within 48 hours. Earlier in the day, the co-conspirator had his backpack stolen by the victim. Later, the suspect (a friend of the co-conspirator) confronted the victim over the backpack, and the suspect ultimately shot and killed the victim. As the suspect fled the scene, he dropped a cell phone onto the sidewalk. Homicide detectives collected the cell phone and brought it to the SDPD Crime Laboratory for examination.



The phone was an older model and had very little data. There was no owner information saved, no photos, and no saved contacts. However, it did contain two text conversations with unsaved numbers that proved to be useful. The first conversation was unrelated to the homicide, but it contained a text message in which the sender addressed the user by his first name. While not a full name, it gave detectives a lead on who the suspect might be. The second conversation consisted of three messages sent from the phone to another number saying, "Leave bro," "Get away," and "Fast," all sent around the time of the shooting.

The phone number that these messages were sent to was determined to be the co-conspirator. Using this information, detectives found the co-conspirator's apartment where they arrested him. They also found the gun used in the crime being stashed in his apartment, as well as a job application filled out by the suspect. Using the information in the job application, detectives were able to track down and arrest the suspect. Thanks to the data found on the cell phone, detectives had actionable information that led to quick arrests. Even with limited data, a little information can go a long way in solving a crime.

Smartwatch Case

A wealthy couple traveling from abroad was staying in San Diego for medical reasons. The couple had 2 children, one infant (the victim) and one slightly older. The couple had hired 2 nannies to care for their children during the trip, one for each child. The family was staying at a large Airbnb on the beach, and each nanny was set up in different rooms. One day, while the couple was out at an appointment, the older child's nanny noticed the infant being fussy, so the infant's nanny (suspect) took him to his room. A little while later, the older child's nanny heard a cry coming from the infant that she had never heard before. She noted the time.



When the couple arrived back at the Airbnb, the mother found her infant son in an unresponsive state, unable to nurse and extremely lethargic. They immediately called 911 and the infant was taken to the hospital. The victim sustained a brain injury and died at the hospital. The suspect was arrested, and her iPhone and Apple Watch were collected as evidence.

During the investigation, the suspect re-enacted how she slammed the victim up and down while holding his ankles. She was confirmed to have been wearing her Apple Watch during the incident.

The suspect's iPhone was extracted and text messages and health data were extensively reviewed. After the older child's nanny heard the strange cry from the victim, the suspect's heart rate spiked at the same time that she noted the time of the cry. In the time frames that the suspect is texting updates to the mother, the suspect's heart rate remains elevated. When the mother arrives home and calls 911, the suspect's heart rate again spikes. It spikes again when paramedics arrive and when they take the victim to the hospital.

The suspect eventually pled guilty.

Arlington Police Department | Death Investigation

Kyle Dishko
Deputy Chief
Arlington Police Department

In November 2023, the Arlington Police Department was dispatched to a Death Investigation at a local hotel. Cleaning staff found a female occupant lying in bed deceased. Officers responded to the location and believed she had overdosed. Under the deceased was a lighter, straw, tin foil, and an M30 pill. The crime scene was processed and a cell phone belonging to the decedent was collected.

An Arlington Police Overdose Response Team detective was assigned the case. Knowing the cell phone was the most important piece of evidence, the detective took the cell phone to the APD Digital Forensics lab. A detective assigned to the lab completed a Full File System extraction using Graykey, and the data was parsed using the Cellebrite Physical Analyzer.

Discovered on the phone were Facebook Messenger chats between the decedent and suspect, text messages between them discussing narcotics sales, photos of pills sent by the suspect, location services showing where the decedent traveled, and Cash App records showing it was opened during the text conversation with the suspect.

In December 2023, the Medical Examiner's Office determined the cause of death was fentanyl toxicity. An arrest warrant for Murder was signed by a judge. The suspect was located and arrested. She was found in possession of Fentanyl pills and a cell phone. A search warrant for the suspect's phone was obtained and the phone was forensically examined. The phone contained the same Facebook Messenger chat with the decedent, evidence the suspect viewed the medical examiners public website about the decedent, and additional drug sales by the suspect.



Core Capabilities (Pages 9-13)

- Casey, E. (2009). Handbook of digital forensics and investigation. Academic Press.
- Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Elsevier.
- Carrier, B. (2003). Defining Digital Forensic Examination and Analysis Tools. Digital Forensic Research Workshop.
- International Organization for Standardization. (2017). ISO/IEC 17025:2017: General requirements for the competence of testing and calibration laboratories.
- Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current Challenges and Future Research Areas for Digital Forensic Investigation. arXiv:1604.03850.
- National Institute of Standards and Technology (NIST). (2014). NIST Cloud Computing Forensic Science Challenges.
- Nelson, B., Phillips, A., & Steuart, C. (2015). Guide to Computer Forensics and Investigations (5th ed.). Cengage Learning.
- Pollitt, M. M. (2010). An Ad Hoc Review of Digital Forensic Models. Proceedings of the 10th Annual Digital Forensic Research Conference (DFRWS).
- Selim, Aybeyan & Ali, Ilker. (2024). The Role of Digital Forensic Analysis in Modern Investigations. Journal of Emerging Computer Technologies. 4. 1-5. 10.57020/ject.1445625.
- Marshall, A. M. (2009). Digital forensics: digital evidence in criminal investigations. John Wiley & Sons.

Legal and Regulatory Considerations (Pages 34-35)

- 1) *Riley v. California*, October 2013, Supreme Court of the United States, Certiorari to the Court of Appeal of California Fourth Appellate District, Division One, No.13-132 Argued April 29, 2014-Decided June 25, 2014.
- 2) *Carpenter v. United States*, October 2017, Supreme Court of the United States, Certiorari of the United States Court of Appeals for the Sixth Circuit, No.16-402 Argued November 29, 2017-Decided June 22, 2018.
- 3) *U.S. v. Hunt*, Supreme Court of the United States, District of Oregon, Portland, In the United States Court of Appeals for the Ninth Circuit, No.23-2342 May 31, 2024.
- 4) *Richardson v. State of Maryland*, September 2021, Court of Appeals of Maryland, No.46 Argued March 3, 2022-Decided August 29, 2022.
- 5) *Commonwealth v. Jones*, Massachusetts Supreme Judicial Court Argued November 6, 2018-Decided March 6, 2019.



Legal and Regulatory Considerations (Pages 36-40)

- 1) <https://www.pewresearch.org/internet/fact-sheet/mobile/> (Pew Research Center, 2024) (*Last Accessed August 2, 2024*)
- 2) <https://worldpopulationreview.com/country-rankings/cell-phones-by-country> (World Population Review, 2019) (*Last Accessed August 2, 2024*)
- 3) *Riley v California*, 573 U.S. 373 (2014)
- 4) *United States v Robert Holcomb* (No. CR21-75-RSL (W.D. Wash. Nov. 8, 2022))
- 5) *New York v Belton*, 453 U.S. 454 (1981)
- 6) *Gustafson v Florida*, 414 U.S. 260 (1973)
- 7) *Riley, supra*
- 8) *Richardson v Maryland*, 481 Md. 423 (Md. 2022)
- 9) Gershowitz, Adam M., "The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches" (2016). Faculty Publications. 1820. <https://scholarship.law.wm.edu/facpubs/1820> (*Last Viewed August 19, 2024*)
- 10) *United States v Joseph Smith* (D.D.C. 19-324 (BAH))
- 11) *United States v Morton*, No. 19-10842 (5th Circuit, 2022)
- 12) *State of Ohio v. Schubert*, 171 Ohio St.3d 617 (Ohio Sup Ct, 2022) (quoting *United States v. Christian*, 925 F.3d 305, 312 (6th Cir. 2019))
- 13) *Burns v United States*, 235 A.3d 758 (D.C. 2020)
- 14) See *United States v Smith*, 22-3015 (D.C. Cir. 2024) ("Without deciding the underlying merits of the claim, we hold that the good-faith exception also precludes [an overbroad] argument") and *Morton, supra*
- 15) See *Richardson, supra*. See also *United States v. Rosa* (626 F.3d 56 (2nd Cir 2010) and *State of Nebraska v Henderson*, 289 Neb. 271 (Neb. S.Ct, 2014)
- 16) See *Burns, supra*, and *Schubert, supra*.
- 17) *Utah v Strieff*, 539 U.S. 232 (2016), quoting *Hudson v Michigan*, 547 U.S. 586,591 (2006)
- 18) Piecemeal, or partial suppression of data – while allowing the admissibility of data for which there was probable cause was articulated by the Massachusetts Supreme Court in *Commonwealth v Snow*, 486 Mass. 582 (2021)
- 19) *United States v. Otero*, 563 F.3d 1127 (10th Cir. 2009).
- 20) *United States v Bishop*, 910 F.3d 335,337 (7th Cir. 2018). See also, *United States v Castro*, 881 F.3d 961,965 (6th Cir. 2018) and *United States v Burke*, 633 F.3d 984 (10th Cir. 2011). *Andresen v Maryland*, 427 U.S. 463 (1976) is also instructive on this topic.
- 21) *Ornelas v United States*, 517 U.S. 690 (1996) (quoting *Illinois v Gates*, 462 U.S. 213 (1983))



San Diego Police Department

Transparent and Responsible Use of Surveillance Technology (SDMC 210.0103(b)(2))

Link: [sd-ordinance-o-2021-69-rev.pdf \(sandiego.gov\)](#)

San Diego Police Department Crime Laboratory Forensic Technology Unit Manual

Link: [1 \(sandiego.gov\)](#)

Scientific Working Group on Digital Evidence

Core Competencies for Digital Forensics

Link: <https://www.swgde.org/23-f-007/>

Best Practices for Personnel Presenting Digital Evidence in Legal Proceedings

Link: <https://www.swgde.org/23-q-001/>

Best Practices for Computer Forensic Acquisitions

Link: <https://www.swgde.org/17-f-002/>

Best Practices for Vehicle Infotainment and Telematics Systems

Link: <https://www.swgde.org/12-f-005/>

Best Practices for On-Scene Identification, Seizure, and Preservation of Internet of Things Devices

Link: <https://www.swgde.org/22-f-001/>

Digital & Multimedia Evidence Glossary

Link: <https://www.swgde.org/05-f-001/>



Acknowledgments

This product was created in partnership and through the efforts, knowledge, and expertise of the individuals listed below. The Major Cities Chiefs Association is grateful for the commitment and work done by this working group and for the time and effort allotted to support and improve the daily operations of law enforcement. This list reflects the authors of the document, however, over forty MCCA agencies participated in information sharing and regular meetings to discuss best practices, challenges, and ways forward in the field of digital evidence.

Katherine Rosoff
Forensic Specialist Supervisor
Albuquerque Police Department

Kyle Dishko
Deputy Chief
Arlington Police Department

Sergeant Bryan Wang
Digital Forensics Lab
Arlington Police Department

Michelle Palamara
Detective
Buffalo Police Department

Major Brendan Hooke
Assistant Commander
Planning and Research Bureau
Fairfax County Police Department

Captain Dana V. Ferreira
Police Liaison Commander
Fairfax County Police Department

Christian Quinn
Managing Principal, Fulcrum Innovation LLC
Deputy Chief of Cyber & Forensics (Ret.)
Fairfax County Police Department

Zachary Johnson
Commissioned Supervisor
Digital Forensics Lab
Las Vegas Metropolitan Police Department

Sergeant Richard Geiger
Technical Services Unit & Digital Evidence Unit
Metropolitan Police Department (Washington DC)

Monica Alnes Niklaus
Director of Projects
Major Cities Chiefs Association

Devin Ross
Detective Lieutenant
Nassau County Police Department
Co-Chair of MCCA Technology Committee

Captain Aaron Busch
Special Operations Bureau
Oklahoma City Police Department

Lieutenant Max Watson
Special Operations
Oklahoma City Police Department

Austin Hartzler
Professional Staff
Computer Forensic Investigations Specialist
Oklahoma City Police Department

J. Bret Aicher
Professional Staff
Computer Forensic Investigations Specialist
Oklahoma City Police Department

Michael Pickle
Professional Staff
Computer Forensic Investigations Specialist
Oklahoma City Police Department

Michael Garvey, PhD
Deputy Managing Director
Philadelphia Police Department
Co-Chair of MCCA Forensic Science Committee

Lisa Merzwski
Supervising Criminalist
San Diego Police Department Crime Laboratory

