PRIORITY
Criminal Justice
NEEDS INITIATIVE
A project of the RAND Corporation, the Police Executive Research Forum, RTI International, and the University of Denver

Digital Evidence and the U.S. Criminal Justice System

Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence

Sean E. Goodison, Robert C. Davis, and Brian A. Jackson

Key findings

- Law enforcement attendees were unanimous in noting the considerable quantity of evidence analyzed by examiners and challenges in obtaining the necessary support, in terms of both funding and staffing.
- Both law enforcement and courtroom participants in our workshop noted potential difficulties with prosecutors not understanding elements of digital evidence. Judges, juries, and defense attorneys also have a stake in appropriate use of digital evidence. Of these, defense attorneys appear to be farthest behind the curve, but are likely to catch up quickly.
- The discussions of the panel identified 34 different needs that, if filled, could improve the capabilities of the criminal justice system with respect to digital evidence. Nine top-tier needs were identified through the Delphi process as highest priority.

Major shifts in the information technology landscape over the past two decades have made the collection and analysis of digital evidence an increasingly important tool for solving crimes and preparing court cases. As technology has become more portable and powerful, greater amounts of information are created, stored, and accessed. Modern devices can serve as huge repositories of personal information yet be carried in a pocket and accessed with a single hand or even voice command. There is a clear benefit to having ample information to obtain convictions, but law enforcement and other criminal justice partners need to balance the recovery and admissibility of digital evidence with privacy concerns. This work discusses the rise of digital evidence, unique challenges, and the results of a workshop held to prioritize needs in digital evidence processing.

INTRODUCTION

While digital evidence exploitation is a relatively new tool for law enforcement investigations, law enforcement relies extensively on digital evidence for important information about both victims and suspects. Due to the potential quantity of digital evidence available, cases where such evidence is lacking are more difficult to develop leads and solve. Three recent investigations illustrate the importance of digital evidence for the criminal justice community—one case presents an example of how digital forensics can be central to case closure and prosecution, another case demonstrates how digital evidence missteps can have serious implications, and the final case highlights the challenges for modern investigation when digital evidence is limited or does not exist.

Abbreviations

CALEA	Communications Assistance for Law Enforcement Act
CCTV	closed-circuit television
ECPA	Electronic Communications Privacy Act
GPS	Global Positioning System
ISP	Internet service provider
IoT	Internet of Things
MLAT	mutual legal assistance treaty
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
PERF	Police Executive Research Forum
PPA	Privacy Protection Act
VoIP	Voice over Internet Protocol

Christian Aguilar

In September 2012, University of Florida freshman Christian Aguilar disappeared after last being seen with his friend, Pedro Bravo, at a local Best Buy (Burch, 2014). Aguilar's remains were found about three weeks later more than 60 miles west in a shallow grave. Police suspected Bravo had something to do with the disappearance and death; searches found some blood in Bravo's car and he was in possession of Aguilar's backpack. Aguilar and Bravo had attended the same high school, and there was a potential motive in that Bravo had been upset that Aguilar had started a relationship with Bravo's ex-girlfriend.

However, digital evidence made this circumstantial case far stronger. Digital examiners had access to Bravo's cell phone and found numerous key pieces of evidence. In the cache for the phone's Facebook app, examiners found a screen shot of a Siri search made near the time of Aguilar's disappearance that read, "I need to hide my roommate." While Bravo's phone did not have the Siri feature, the record was maintained because he used Facebook to access the option. Analysis of pings, or determining the tower that received a signal from the cell phone, showed that Bravo had headed far to the west after the disappearance. Finally, examiners were able to determine that the flashlight application on the phone had been used for over an hour just after the disappearance. As a result of this evidence, Bravo was brought to trial in August 2014 and convicted of first-degree murder.

Casey Anthony

The murder trial of Casey Anthony in 2011 captured national media attention in the United States. Anthony reported her two-year-old daughter, Caylee, missing in 2008. She claimed Caylee was last seen being dropped off with a babysitter, though she did not report the incident to police until over one month later. The State of Florida arrested Anthony on charges of child neglect, false statements, and obstruction. As the police investigation continued, physical evidence from Anthony's car suggested potential homicide, which led to a grand jury indicting her on murder charges as well. Months after the indictment, Caylee's remains were found in a wooded area near her home.

During trial, the state argued that digital evidence would prove Anthony searched for information on various homicide-related issues (methods, techniques, etc.) on the day her daughter was last seen. Most such evidence focused on Internet browser searches. Digital investigators initially used software that later would be found highly inaccurate (Alvarez, 2011). Investigators testified that Anthony's browser searched 84 times for "chloroform," a chemical that had been found in her car trunk; however, the software designer later discovered serious faults in the program and subsequently testified that the term was only searched for once. This error likely contributed to the reasonable doubt jurors found when they acquitted Anthony of first-degree murder, especially since the correction occurred during trial.

Interestingly, further evidence came to light in the years after the trial to suggest more digital evidence mistakes that served to further weaken the case. Investigators used tools that only tapped into Microsoft's Internet Explorer history. While technicians determined the computer was being used through a password-protected account of Anthony's, thus strongly suggesting it was Anthony and not other family members using the computer, they missed that Anthony preferred Mozilla's Firefox browser with their software; as result, investigators did not have information on more than 98 percent of the browser history records at trial, including a search for "foolproof suffocation" (Pipitone, 2012).

Philip Welsh

Philip Welsh was murdered in his home in Silver Spring, Maryland, in February 2014 (Morse, 2014). He worked as a taxicab dispatcher for many years, and in the workplace he used computers and technology daily. However, he eschewed

all digital devices in his private life. Welsh did not own a cell phone or computer, instead relying on landlines, typewriters, and hand-written letters. Even his television was an older, cathode ray tube model. By all accounts, Welsh was perfectly happy without modern technological devices—friends and family would prompt him to try a new device or the Internet but Welsh preferred nondigital technology.

Welsh did not report for work one day and was found murdered in his home. He lived alone and had no known enemies; in fact, he was well-liked and often left his home open to taxi drivers who needed a place to sleep between shifts. With a limited pool of leads, the lack of digital evidence was even more noticeable. Investigators have no ready way to determine what Welsh's activities were or who he met without evidence like text messages, email, and web history. As of this publication, the murder of Philip Welsh remains unsolved and officials note that this is in considerable part due to the lack of digital evidence.

The Nature of Digital Evidence

Digital evidence is conceptually the same as any other evidence—it is information leveraged in an attempt to place people and events within time and space to establish causality for criminal incidents. However, digital evidence has a wider scope, can be more personally sensitive, is mobile, and requires different training and tools compared with physical evidence. This section incorporates a general classification system to understand types of digital evidence and techniques for extracting data from digital devices.

Digital evidence is "information and data of value to an investigation that is stored on, received, or transmitted by an electronic device" (National Institute of Justice [NIJ], 2008).[1] While such evidence has existed for decades in limited forms, such as mainframe computers and telephonic systems, the importance of processing digital evidence has increased with the rapid proliferation of personal electronic devices. The 21st century has been partially defined by advances in portable music players, cell phones, and computing devices. The U.S. Supreme Court recently noted that cell phones are not simply communication devices, but rather microcomputers that can serve as a telephone, calendar, diary, and email system; the "element of pervasiveness that characterizes" modern technology (see the discussion of *Riley v California* later in this section) results in three characteristics central to understanding how digital evidence differs from traditional physical records and evidence: (1) Digital evidence has a wider scope, (2) it deals with both physically and personally sensitive information, and (3) it taps into interconnected criminal justice issues that go beyond law enforcement's typical role in collecting evidence.

Types of Digital Evidence

The wide range of digital devices and extraction processes yields a commensurate potential for recoverable evidence. We briefly note the most common outcomes from digital evidence processing. This listing is not exhaustive but does touch on the major areas of evidence, providing both a picture of the range of ways digital evidence can affect criminal justice and the potential challenges faced by agencies in collecting, analyzing, and utilizing it.

Internet

Some of the first digital evidence used in law enforcement investigations came from communication websites, particularly message boards and chat rooms. These types of sites continue to be a source of information for current investigations, though the proliferation of other Internet and Internet-enabled technologies means that they are now numbered among many potential sources of evidence. Both message boards and chat rooms allow users to read and respond to chains of communication either as an archive or in real time. There are a number of law enforcement challenges in using these sources. The locations and addresses of such sites are not always public knowledge, meaning that initial intelligence

Digital evidence has a wider scope, can be more personally sensitive, is mobile, and requires different training and tools compared with physical evidence.

work or online searching may be required to find the sites. Users rely on anonymity and potentially encoded or encrypted communications to prevent most readers from understanding the communication and identifying the participants. The worldwide nature of the Internet complicates this, as even a successful identification may yield an individual outside the investigator's jurisdiction. Still, these sites can provide useful intelligence and indicate linkages between participants.

File-sharing networks are another major source used during investigations. These networks connect users to transfer data files, such as pictures and video. Numerous major file-sharing networks have been shut down or revamped following law enforcement investigations and legal action, particularly in reference to copyright violations and the exchange of other illegal materials. Users can be tracked, and downloaded files can often be linked to specific IP addresses. For example, a music copyright case may be less concerned with a specific music file than it is with the statutory violation of the copyright and with which users participated. However, the content of the transfers can also be relevant to a case, such as in child pornography investigations.

Some Internet technologies have been designed specifically to enable hiding the identity and location of individuals who are accessing or sharing information. For example, the Tor Project provides a high degree of anonymity for Internet users. Developed through funding primarily from the U.S. government, the Tor Project was designed to enable safer Internet access by individuals in countries with considerable censorship or repressive regimes. However, the system is now used worldwide to mask legal and illegal activities though Tor's "onion" security protocols that encrypt information multiple times over. Some major illegal activities using Tor, such as the Silk Road trading site that featured a wide market of illicit drugs, have been shut down by law enforcement in recent years. These types of sites are part of the Deep Web, which is the area of the Internet not covered through standard search engines like Google or Yahoo.

Some Internet technologies have been designed specifically to enable hiding the identity and location of individuals who are accessing or sharing information.

Computers

There is a wealth of potential digital evidence on a personal computer. Many of these items can be obtained through a manual or logical extraction process. While some of the evidence overlaps with information found online, there are a few notable sources that can be found on a physical device rather than on the Internet.

When browsing the Internet, programs will often maintain temporary Internet files, cookies, and a browsing history. Each of these items can be used in an investigation to determine the user's web activity. In fact, temporary files and cookies are typically used by websites themselves to track users and store information.

Email and other messages may be found on the physical computer as well. Though most email is held on Internet servers—which themselves can be a target of law enforcement, as seen in recent court cases against Google and Microsoft—some messaging software archives prior messages onto a computer hard drive.

Portable Electronics

Currently, digital evidence processing from portable electronics such as cell phones is the primary focus of interest to examiners and researchers. Within the past decade, the use and power of such devices has increased drastically, leading to mass-marketed small electronics containing potentially more-personal information than any prior combination of electronic and physical sources, all in one portable device.

There should be no surprise that cell phones are the dominant interest within the field of digital evidence. These devices are nearly ubiquitous in our modern society, have undergone a revolution of capabilities during the 21st century, and present new legal challenges such that the U.S. Supreme Court recently ruled that a warrant is required for most searches of cell phones at a scene. According to industry surveys, the number of wireless subscriptions in the United States currently exceeds the total population (336 million subscriptions to 313 million population); this subscription estimate is more than double the

count from ten years ago of 159 million (*Annual wireless industry survey,* 2014). As Chief Justice John Roberts noted in the *Riley* decision, cell phones are "microcomputers" that serve a large number of critical uses for people. This is one reason why the Court ruled that law enforcement must have a warrant to search cell phones at a scene—unlike a piece of paper or other portable item, the information within a cell phone could be equivalent to large, nonportable items, such as ledgers, diaries, or personal computers. Additionally, cell phones have standard features allowing for photography, Global Positioning System (GPS) location, and text messaging distinct from email or other documents. These features nearly eclipse that a cell phone is also a telephone, which often has a contact list, log of calls made and received, and call duration.

As technology progresses, portable electronics will be central in the Internet of Things (IoT) due to increased connectivity and integration. IoT generally refers to the interconnection of electronic devices to share a greater range of data (e.g., sensory inputs rather than simply manual entry) and provide automation of other tasks associated with electronics (e.g., controlling one's DVD remotely or making changes to robotic factory lines). Portable electronics would serve as an input and output device, taking in environmental information and time-stamping changes while also providing users control over a wide array of other technological processes. In terms of digital evidence, the advancing power and storage in portable electronics suggest that connection with an IoT would result in far more data than seen currently, which could be both a blessing and curse for investigations—automation could provide key evidence that may be difficult to alter or destroy, but the quantity of information could possibly overload investigative resources.

The first wave of this interconnected information involves uses of metadata, or detailed information about a particular piece of digital data such as a picture or document. Metadata provides an additional layer of encoded information within the main file. Examples of metadata are time stamps, geospatial information, or even copyright information. Often, the inclusion of metadata is automatic on mobile devices though there are options to disable encoding. Such data have clear evidentiary value for investigations but can also tap into privacy concerns, given the range of additional information. Additionally, this data can be altered either directly or remotely by a knowledgeable technology consumer—as a result, investigation protocols will need to become more sophisticated as strategies shift focus onto metadata validation.

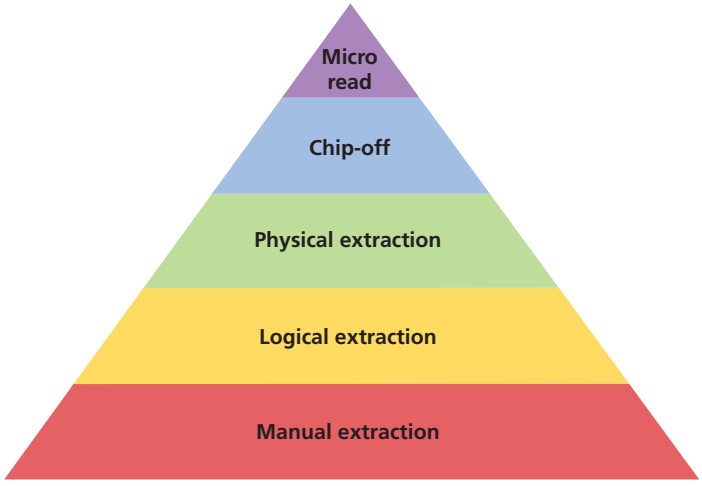
Extraction Techniques

Though initially created to describe mobile extraction tools (see National Institute of Standards and Technology [NIST], 2013), the hierarchy shown in Figure 1 is also useful to understand the challenges posed by digital evidence extraction generally. Each stage in the figure requires a different skill set and equipment and may yield evidence not obtainable through any other stage. Extraction is not simply scrolling through text messages or copying files from a hard drive, though such activities often represent the first stage of the extraction process.

Manual techniques involve using standard inputs included with or built into the device, such as touch screens or keyboards. This is the most basic level of extraction as it does not require specialized tools, though knowledge of file structure and operating systems will aid considerably in analysis. Manual extraction allows access only to information available through the standard interface. For example, deleted items would not be obtainable through this process, as deleted file clusters cannot be explored through basic point-and-click operations. This level of processing is comparable to sitting at a computer looking for a particular file by exploring file folders with a mouse and keyboard.

Logical extractions incorporate external computer equipment to provide commands through code to the targeted device. Examiners can use a number of different connection tools and software products to communicate with the device through the examiner's computer, where extracted data would appear. This level of processing is comparable to using a DOS prompt to control a computer rather than a modern operating system. More precise control is available at the coding level, but

Figure 1: Digital Evidence Extraction Scheme



SOURCE: NIST, 2013.

RAND *RR890-1*

> Departments face large digital evidence backlogs, limited equipment, and potential turnover of examiners.

it also requires considerably more knowledge and sophisticated tools.

Physical techniques refer to reading information from flash memory sources. Flash memory is where a device stores a history of actions to read or write information. Digital evidence at this level can tap into deleted information. There is additional difficulty in accessing flash memory and decoding it, as the data stored here is primarily for the internal working of the device in binary rather than information intended for human observation. A rough comparison would be if one had access to a keylogger to note previous inputs into a computer, as well as a global undo or recovery function that would allow recreation of deleted information. Needless to say, this level requires more knowledge and tools than previous levels, but the potential evidence is both greater in quantity and more difficult for a suspect to alter.

The final processing options, chip-off and micro read, are highly technical activities and represent advanced digital evidence extraction.[2] Both involve a physical removal of flash memory chips from the device. Attempts to read the stored information are done directly with the memory chip and not through the device, so the examiner needs to know proprietary details regarding communication with the chip and needs to simulate the device's communication process. These options are similar to a microscopic examination of components or to making a physical extraction of a hard drive, though hard drives are far easier to access and generally provide output in known, nonproprietary formats by default.

From the perspective of a law enforcement department, the range of extraction modes that can be required to obtain digital evidence from different sources or types of devices means that its collection and use is truly a multifaceted challenge, potentially requiring building and maintaining a variety of quite different technical capabilities and expertise.

In This Report

Many departments are behind the curve in handling digital evidence. The explanation for this deficiency touches on a number of factors, including rapid changes and proliferation of digital devices, budgetary limitations, and lack of proper training opportunities. Departments face large digital evidence backlogs, limited equipment, and potential turnover of examiners through frustration or even being promoted out of the unit. Another important issue is the lack of consensus regarding the needs in digital evidence processing. Without an ability to assess current best practices and prioritize the next steps for effective processing, targeted solutions to problems and weaknesses are impossible.

This report is one product arising out of the broader NIJ-funded research effort focused on identifying and prioritizing needs for innovation and improving performance in the U.S. criminal justice enterprise. The overall effort is charged with identifying needs—things that could be done in technology, policy, practice, or training that could improve performance in criminal justice agencies. This larger effort is rooted in an attempt to understand existing performance; the supply of technology, policy, and practice already available in the community; and how emerging trends in society, technology, and knowledge might affect performance going forward. In an effort to frame an innovation agenda for criminal justice to guide decisionmaking by government agencies, research funders, and the private sector, the project is developing systematic ways to prioritize the many possible opportunities for innovation that are identified.

The following sections present our assessment of the current state and needs within digital evidence processing. Our review of the research and legal literature provides a snapshot of the digital evidence field, an area that has had rapid growth yet has many unanswered questions and unfulfilled needs. These findings set the framework for our digital evidence workshop; the primary goal of the workshop, which brought together subject-matter experts on digital evidence technology and policy, was to build on needs found during our literature review and uncovered through the workshop discussion, and to systematically prioritize the resulting innovation options. The participants highlighted many expected difficulties, such as workload and storage issues and resistance to transitioning away from federal funding streams. In the end, we have a comprehensive listing of prioritized needs that can assist in moving digital evidence processing innovation forward.

THE STATE OF DIGITAL EVIDENCE TODAY

Given our current digital society, the concept of digital evidence is expansive in scope. The most obvious example is the wide range of devices that can contain digital evidence. Digital evidence examiners must be able to retrieve information from various models of cellular phones (e.g. Android, Apple, and Blackberry), desktops, laptops, tablets, external storage devices, GPS locators, and various other devices. The listing and variety of products pose challenges because there is no uniform process to obtain information across makes and models, let alone different types of devices.

Digital evidence can come from both suspects and victims, as all involved parties may have their own personal devices that are relevant to the investigation—in modern society, it is likely both parties would have their own cell phones, which could be used to ascertain what each was doing before the crime, who each party contacted, and if there was any previous interaction. Evidence pointing toward guilt, such as threatening messages, may be commingled with exculpatory evidence, such as time-stamped pictures far from the crime scene. Given the required time and effort to extract and sift through information from a single device, the investigative workload can easily double when each party has a cell phone or other electronic item. Additionally, there are considerable jurisdictional issues that expand the potential scope of an investigation. Electronics connect the world and cross borders, whether it be through the Internet, social media, or even cloud storage. In these cases, the digital evidence required for an investigation may not exist primarily on a physical device but rather on a server many counties, states, or countries away.

Digital evidence tends to involve sensitive information, both physically and personally. Modern electronic devices, trending smaller and more lightweight to aid in mobility, can also be fragile. As a result, digital evidence can be damaged or altered by basic actions, such as dropping an item in water, passing a powerful magnet by it, or even through sheer physical force to break components.[3] From a personal standpoint, cell phones and other digital devices raise significant privacy concerns because they tend to hold a far greater quantity of information on lifestyle, associates, and activities beyond the specific evidence needed for investigation. The collection and processing of digital evidence have implications that expand beyond the traditionally more linear role of law enforcement to obtain evidence. Digital evidence collection is not solely about using new technology internally to extract information, but also the need of law enforcement to continuously react to changing technology externally. Methods and tools from ten years ago are often insufficient and incompatible with current technology. This turnover is due to the rapidly changing landscape of personal electronics. Law enforcement must not only *be* up to date, it must *stay* up to date regarding new devices and new techniques in order to best assist investigations. Due to modern phones being microcomputers, the rules of search and seizure have changed, to say nothing of the investigative changes needed to analyze a device with more storage and power than desktop computers (e.g., more man-hours, sophisticated equipment, potential to find additional information not covered by an initial warrant, and requirements to search and report exculpatory evidence).

Research Assessing Digital Evidence

One large domain of digital evidence is the search and analysis of websites for traditional investigations. Investigations in crimes such as child pornography and the sex trade predate the digital evidence area; however, new avenues opened as result of the growing use of the Internet as a communication medium with global reach. While this first area of digital evidence use is the oldest, it remains durable as law enforcement continues to investigate sex crimes coordinated or conducted over the Internet. Work on the *Wonderland Club*, a global child pornography ring (Graham, 2000), and more-recent usage of Craigslist and other online forums to organize prostitution

Digital evidence collection is not solely about using new technology internally to extract information, but also the need of law enforcement to continuously react to changing technology externally.

Digital evidence examiners have used sites such as Facebook and MySpace for traditional investigation to establish timelines and peer-group linkages. However, more evidence exists on both the local device accessing social media and on the social media servers themselves.

(see Latonero, 2011) represent the case-study approach often used by the literature in this area. Many of the same issues first introduced through this topic area remain relevant today. Questions regarding how to trace evidence (e.g., pictures) back to the source, admissibility in court, policies dictating searches of people and/or devices, jurisdiction, and entrapment first surfaced within the context of investigating Internet pornography and remain some of the key concerns moving forward.

Another topic area includes tools and techniques to obtain information from hardware. Literature within this area started to develop in earnest in the mid-2000s, punctuated by two major "how-to" guides funded by the federal government (see NIJ, 2007a; 2007b; 2008). Recently, the main focus has been on cell phones. NIST produced a comprehensive report on modern mobile devices (NIST, 2013) to augment the techniques described in the earlier NIJ reports. NIST is a part of the U.S. Department of Commerce and serves as a major physical science laboratory and source of measurement standards for the nation. NIST is among those collaborating with NIJ to develop equipment standards for criminal justice agencies. Additionally, NIST has contributed to establishing forensic science standards in a large set of fields, such as firearm examinations, questioned document reviews, polygraph examinations, arson investigations, and others. In September 2014, NIST established a digital evidence subcommittee tasked to "identify and develop national standards and guidelines for forensic science practitioners" (NIST, 2014). This follows numerous reports and hosted conferences to discuss best practices for data extraction from mobile devices (see NIST, 2013). These actions indicate that NIST will be a key agency in continuing research and developing standards for digital evidence processing.

While federal intervention sought to provide general guidance, independent research into hardware extraction sought to evaluate different commercial techniques and products. For example, Mutawa, Baggili, and Marrington (2012) evaluated the forensic potential of the three major cell phone operating systems, Android, Apple, and BlackBerry. The authors found that social networking applications left significant amounts of data recovered through logical extraction on Apple and Android phones, but not BlackBerry.

A third topic area encompasses tools and techniques to retrieve digital evidence from IT systems. In a way, this is a hybrid of the first two topic areas, in that evidence from IT systems may be stored on local hardware (computer, phone), an external fixed server, or in cloud servers potentially in multiple locations. Evidence can be accessed locally but stored remotely, which causes new difficulties for digital extraction. This area is the newest topic and is only starting to develop a basic knowledge base. The limited literature to date tends to focus on either social media or cloud storage, and typically on services only "one hop" from a user.

For social media, digital evidence examiners have used sites such as Facebook and MySpace for traditional investigation to establish timelines and peer-group linkages. However, more evidence exists on both the local device accessing social media and on the social media servers themselves. Cusack and Son (2012) found that while numerous tools exist to extract evidence from social media, the functionality can vary greatly and best results may depend on what the examiner is specifically looking for, such as postings or chat logs.

Zawoad and Hasan (2013) note that there are critical forensic problems with the cloud, such as physical inaccessibility, data of numerous individuals commingled, and chain-of-custody issues where the server location is unknown (see also Ruan, 2011). Delport, Köhn, and Olivier (2011) examined multiple methods to isolate cloud data for extraction, with mixed results similar to Cusack and Son's attempt at social media sites—different tools have different strengths and weaknesses, though Delport Köhn, and Olivier concluded that a combination of techniques may be best for now and that future tests are required.

Research has focused on direct link or "one hop" applications where users input a degree of data but often end up sharing more than intended due to metadata and corporate data mining—for example, Facebook uses targeted ads based on user data and Google provides similar ads through analysis of Gmail contents. However, other services can collect, compile, and mine personal data indirectly, such as apps that ask for specific permissions to run on a cell phone. Such indirect services, like games or GPS tools, could also provide similar information for purposes of an investigation and likely represent a new avenue for digital evidence moving forward.

Legal Issues Involving Digital Evidence

With constant changes in technology, law enforcement must draft up-to-date policies to address digital evidence issues. In order to establish policies, law enforcement must also work with other partners, such as the courts and prosecutors, to determine legal requirements regarding chain of custody and admissibility. Evidence is of little use to the criminal justice system when it is ruled to be improperly obtained after the fact.[4] Law enforcement and its partners need to have a consistent set of expectations and deliverables for digital evidence, which can prove to be different from the process and policies for nondigital evidence. Here, we review the legal issues in the United States, for both law enforcement and the courts, related to digital evidence. The following discussion draws on material from an NIJ report (2007a) on use of digital evidence in the courtroom, a Powerpoint presentation by Degani (2014), and unpublished work by Fakhoury (2015).

Search and Seizure Issues

The Fourth Amendment provides protection against unreasonable search and seizure by governmental authorities. Courts have been coming to grips with the unique nature of digital devices and digital information and interpreting how the Fourth Amendment should apply to digital information. In cases where the Fourth Amendment applies, law enforcement officers must obtain a search warrant from an appropriate court in order to carry out a search, although some exceptions apply. Warrantless searches may be carried out with consent of an appropriate party. Exigent circumstances, or immediate danger of destruction of evidence, can also be cause for a limited search of an electronic storage device. Limited searches may also be carried out in the context of arrest, when necessary to protect law enforcement officers or prevent the destruction of evidence.

Evidence in plain view of officers may also qualify as an exception to the search warrant requirement (*Horton v California*, 1990).[5] However, application of this principle becomes complicated in the case of electronically stored information. Murphy and Esworthy (2012) recommend viewing collection of electronic evidence via search warrant as a two-stage process. The first stage is the seizure of the device or devices on which the information covered by the warrant resides. According to Murphy and Esworthy, courts have recognized that the initial seizure may, of necessity, be overly broad and include much information not covered by the search warrant. Therefore, there needs to be a second stage in which law enforcement agents examine the data seized and cull the information specifically covered under the search warrant. This requires examining files on the seized devices: In the course of such an examination, additional evidence of criminal activity may be uncovered that is outside the scope of the search warrant. Courts historically have questioned whether such material is covered under the plain view exception.

One influential decision (*United States v Comprehensive Drug Testing, Inc.*, 2009) recognized that over-seizure is inherent in cases involving electronically stored evidence and everything seized could be construed to be in "plain view" as files were examined. Therefore, the court ruled that certain requirements must be followed by law enforcement, including (a) reliance on the plain rule exception must be waived; (b) search protocols should be used that are designed to uncover only the information for which law enforcement has probable cause; (c) segregation of nonresponsive materials must be done by parties other than the case agents; and (d) the government must return or destroy nonresponsive

With constant changes in technology, law enforcement must draft up-to-date policies to address digital evidence issues.

> Congress has passed numerous laws to balance the requirements of the Fourth Amendment and the needs of criminal investigations.

data. However, a differing opinion was rendered by the Fourth Circuit (*United States v Williams*, 2010) stating that since computer searches must include viewing each file on the device, the criteria for applying the plain view exception are met. According to Murphy and Esworthy, current judicial thinking is tending toward greater restriction on what is included in searches of electronic devices.

In the United States, Congress has passed numerous laws to balance the requirements of the Fourth Amendment and the needs of criminal investigations. Four portions of the U.S. Code are particularly relevant to digital evidence: the Wiretap Act (18 U.S.C. §2510 et seq.); the Pen Registers and Trap and Trace Device Statute (18 U.S.C. §3121 et seq.); the Electronic Communications Privacy Act (ECPA) (18 U.S.C. §2701 et seq.); and the Privacy Protection Act (PPA) (42 U.S.C. §2000aa et seq.).

The Wiretap Act protects the parties to a wire, oral, or electronic communication from having that communication intercepted by a party external to the communication. The act applies to bugs designed to eavesdrop on oral communications, telephonic voice and text messages, or computer-generated messages such as instant messages or email. With strong justification, a court may issue an order authorizing interception by law enforcement. Government efforts to intercept communications without a court order can result in civil or criminal penalties and suppression of evidence.

The Pen Registers and Trap and Trace Device Statute restricts collection of metadata concerning telephone and Internet communications. Unlike the Wiretap Act, which governs the content of communications, the Pen/Trap Statute covers information such as email addresses and phone numbers dialed or phone numbers of calls received. If no exception to the statute applies, law enforcement officers must seek a court order prior to seeking communications metadata.

The ECPA contains a provision dealing with records and files stored by service providers. It protects email and other subscriber data stored by Internet service providers (ISPs) from disclosure without appropriate legal authorization. The kind of authorization required by law enforcement to access stored information ranges from subpoena to court order to search warrant, depending on the sensitivity of the information sought. The act does not apply to communications information stored on suspects' own computers. Developing law is suggesting that overly broad civil subpoenas may not be sufficient to compel ISPs to provide private information of users (Murphy and Esworthy, 2012). However, ECPA considers material stored on a third party's server for more than 180 days to be abandoned, so that law enforcement personnel only need to provide a written statement certifying that the information is relevant to an investigation. Users today are likely to store email on third-party servers indefinitely, which gives law enforcement a huge advantage since they would otherwise need a warrant to obtain the same information from the user's personal devices. There has been substantial debate about eliminating the 180-day rule.

The PPA protects products created by an author (such as online newsletters or blogs), as well as materials used in the creation of that product. Materials covered under PPA are not subject to search warrants. However, exceptions apply when the materials are connected to commission of a crime or when their seizure would prevent death or serious bodily injury.

In addition, the 1994 Communications Assistance for Law Enforcement Act (CALEA) was designed to facilitate efforts by law enforcement to conduct surveillance of telephone networks. The act required telephone companies to redesign their network architectures to make such surveillance easier. While it expressly excluded the regulation of data traveling over the Internet (Electronic Frontier Foundation, undated), the FCC ruled that CALEA could be expanded to Internet broadband providers, like ISPs, and certain Voice over Internet Protocol (VoIP) providers. Supporters of CALEA argue that it helps reduce the effort by law enforcement to develop ways to keep up with technological privacy innovations. Detractors worry that use of the law will continue to be expanded at the expense of individual privacy.

In 2014, the U.S. Supreme Court rendered a potentially game-changing decision on search and seizure of cell phones in the course of making an arrest. In *Riley v California*, the Court ruled unanimously that warrantless search and seizure of digital contents of a cell phone made during the course of an arrest are

unconstitutional. The decision ended contradictory opinions issued by several circuit courts and state supreme courts about whether warrantless cell phone searches were allowable under an earlier Supreme Court decision. That decision permitted police to search the body of an arrestee without a warrant in order to protect material evidence or officers' safety. In the Court's opinion, Chief Justice Roberts wrote:

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life." The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.

Riley establishes a rule for searching digital evidence that is separate from rules for searching physical evidence. It recognizes that the quantity of data and qualitatively different nature of some digital data (for example, GPS location) necessitates a different application of the Fourth Amendment (Kerr, 2014a).

Riley makes on-scene triage more challenging. When an arrest is made, there is a possibility that a confiscated cell phone could be wiped via a remote command, or timed security locks could be activated resulting in loss of access to data. Some digital forensic laboratories have provided mobile forensic field kits for on-scene inspections performed by less-technical digital investigators (Mislan, Casey, and Kessler, 2010). *Riley* makes on-scene triaging more difficult by requiring a warrant before proceeding to extract data from cell phones. The Supreme Court decision acknowledged that destruction of data may, at times, occur, but argued that the time to obtain a warrant would not add significantly to this danger. In a related Supreme Court decision (*United States v Wurie*) the Court reaffirmed the requirement for a warrant to search cell phones, but provided an exception for exigent circumstances.

Jurisdictional Boundaries

In trying to recover digital evidence from ISPs, law enforcement officers frequently find that the information sought resides with providers located out of state or even internationally. Regarding states, some require that entities within their state comply with extrajurisdictional processes, but most do not. In the latter situations, an ISP may balk at complying, especially out of fear of incurring liability under the ECPA. In situations where an ISP refuses to comply with an extraterritorial search warrant, law enforcement officers have the option in some instances of seeking a trial or grand jury subpoena that may be more effective in inducing compliance. Alternatively, law enforcement officers may seek to have a warrant prepared by officers in the ISP's home state based on an assertion of probable cause. International warrants can be complicated by the necessary mutual legal assistance treaty (MLAT). Agencies cannot directly serve international sources, but rather work through the MLAT process to ensure that legal requirements in each country remain satisfied.

Documentation

Documentation of digital evidence incorporates the twin issues of *authentication* and *chain of custody*. Authentication is the process of establishing that the evidence is actually what its proponents claim it to be. The party putting forth the evidence is required to demonstrate that the item is genuine. A key issue in authenticating digital evidence often involves establishing the identity of the author of electronic records. For example, a prosecutor would need to show proof that an email allegedly written by a defendant to a victim actually was drafted by the defendant. The Federal Rules of Evidence, also adopted by many state courts, allow that authentication may be established via testimony of a knowledgeable witness, such as a law enforcement officer who seized a computer or cell phone who is able to testify where the files were taken from and matches of names in the files to other evidence collected. Email may be authenticated through a variety of means, including establishing that the email contains information the defendant would have been

Documentation of digital evidence incorporates the twin issues of *authentication* and *chain of custody*.

familiar with or testimony that the defendant had primary access to the device on which the message was produced.

As part of the authentication process, chain of custody assures that digital evidence has been preserved in its original form. This entails being able to document when the evidence was collected and where it was collected from (i.e. type, identity, and ownership of device), who owned the device, and who had access to it. It also entails how the evidence was collected (i.e. what tools and procedures were used). Finally, chain of custody involves documenting how the evidence was stored, who has handled the evidence, and who had access.

Hearsay

The rules of evidence include a preference for witness statements introduced in live testimony in the courtroom where the appearance and behavior of the witness can be assessed and the witness can be subjected to cross-examination. Testimony given by witnesses based on conversations held outside the courtroom are considered "hearsay." Some digital evidence falls under the heading of such hearsay statements. However, there are many exceptions to the hearsay rule, and digital evidence often is exempted under one of these exceptions. One exception to the hearsay rule is an opposing party's statement (Federal Rules of Evidence 801[d][2])—for example, statements made by the defendant that are preserved in text messages, email, or other digital media.

Admissibility

An important evidentiary issue with respect to digital evidence is reliability. The Federal Rules of Evidence 702 require that scientific and expert testimony must be reliable both with respect to the principles and methods used by the expert and application of the principles and methods to the specific facts. The original test for admissibility of scientific evidence was the Frye test (*Frye v United States*, 1923). The Frye test allowed scientific evidence to be admitted if the science upon which it rested was generally accepted by the scientific community.

More recently, the Frye test has been replaced in federal courts by the *Daubert* test (*Daubert v Merrell Dow Pharmaceuticals*, 1993). *Daubert* held that the courts have a gatekeeping obligation to assess reliability of scientific evidence. The Supreme Court proposed five criteria to determine the admissibility of scientific evidence: whether the technique has been tested, whether it has undergone peer review, whether there is a know error rate, the existence and maintenance of standards controlling its operation, and (like Frye) whether the technique is generally accepted by the scientific community.

The work of NIST is, for this purpose, very important. The field of digital evidence—both the devices to be exploited and the tools to exploit them—change rapidly. NIST testing provides the basis for asserting that the data gathered and analyzed by new tools is scientifically valid.

New advances in computer forensics technology will continually raise reliability issues, particularly as new techniques are deployed in the field without extensive review and testing seen in nontechnological scientific fields. For example, one federal district court has found that testimony about the "granulization" theory of historical cell site data was not reliable enough to pass *Daubert* (*United States v Evans*, 2012). The court believed that an FBI agent could give lay opinion testimony about the location of cell phone towers in a particular area and the specific towers that an individual defendant connected to, as well as expert testimony about how cell phone technology works.[6] But the agent could not testify about his opinion about the actual location of the phone, since there was significant dispute about whether a cell phone typically connects to the closest cell phone tower.

Obligations to the Defense

Finally, law enforcement has discovery obligations that require them to provide certain forms of evidence to the defense. The

Digital Evidence Workshop Participants (Excluding NIJ, PERF, and RAND Staff)

Stephen Larsen, Suffolk County (NY) Probation Department
Jeff Cotner, Dallas (TX) Police Department
Margery Lexa, Florida Attorney General's Office
Shawna Coxon, Toronto Police Department
Sean Lips, Milwaukee (WI) Police Department
Karen Lissy, Research Triangle Institute
Doug Elrick, Digital Intelligence
Steve Litwin, San Diego County (CA) Sheriff's Office
Bryant Fair, Baltimore (MD) Police Department
Kevin McNamara, San Diego (CA) Police Department
Hanni Fakhoury, Electronic Frontier Foundation
Mike Salter, Ramsey County (MN) Sheriff's Office
David Sun, Sunblock Systems
Greg Guillette, Palm Bay (FL) Police Department
Mike Weaver, Arlington (TX) Police Department
Steven Jansen, Association of Prosecuting Attorneys
Mike Yu, Montgomery County (MD) Police Department

obligation to turn over both exculpatory evidence under *Brady v Maryland* (1963) and impeachment evidence under *Giglio v United States* (1972) means law enforcement may need to scour through digital media it has in its possession, whether social media information or data on a hard drive or phone. Discovery obligations are not just limited to *Brady*. Forensic examination reports must be turned over as well.

When it comes to turning over digital evidence to the defense, law enforcement and prosecutors must be diligent to ensure that the discovery is not only usable but given in a timely manner to defense counsel. In one particularly egregious example, a federal court in Miami ordered a new trial after prosecutors turned over more than 200 pages of Skype logs to impeach a defendant who had just testified. Though the defense had previously been given an image of the hard drive, the chats that prosecutors planned to use were in a format the defense could not open and would need to hire a forensic examiner to review. In granting a new trial, the federal judge noted that the discovery to the defense was not "made in a reasonably usable form" but instead was done in a way "that disguises what is available, and what the government knows it has in its arsenal of evidence that it intends to use at trial" (*United States v Stirling*, 2012).

Summarizing the Legal Issues

Digital evidence has quickly grown from a limited field to one that is often the focus of criminal investigation and associated litigation. The primary focus on digital evidence today is cell phones, though the practical scope is far wider than one category of device. This rapid ascent, coupled with the faster change and development of technology itself, has led to a current state where the field has more that is still to be determined rather than already known. Moving forward, issues relating to cloud-based information and legal challenges associated with the proper scope for searching portable electronic "microcomputers" will shape the future of digital evidence processing.

The fast-moving nature of this field is evidenced in a recent challenge to exploiting digital evidence on cell phones this year when Apple announced that its new iOS 8 operating system has improved security that prevents Apple from unlocking phones even in response to a request from law enforcement. On phones using the new operating system, photos, messages, email, contacts, call history, and other personal data are under protection of a passcode that Apple is not able to bypass. Google has announced that it will do the same in new Android-based operating systems. Some have argued that this may not pose a huge barrier to search warrants since Apple can still provide data stored in its data centers that contain nearly all of the data contained on the users' phones (see Leyden, 2014).

However, Kerr (2014b) argues that this is potentially a major challenge to digital forensic examiners. Kerr argues that what Apple has done in effect thwarts lawful search warrants, contrary to the public interest.[7] He suggests that the inability to obtain access to data once a phone is locked will lead to new questions about the exigent circumstances exception to obtaining a search warrant: Will police officers begin to search unlocked cell phones claiming exigent circumstances when they make an arrest, knowing that once the phone is locked, data is unobtainable? Kerr proposes several legislative solutions to the problem of unbreakable passcodes, including (a) requiring cell phone manufacturers to provide a technical means to bypass passcodes (as recommended by the Commission on Accreditation for Law Enforcement Agencies); (b) penalties for arrested persons who refuse to provide a passcode; and (c) requiring cell phone companies to store and retain data found on users' phones. Kerr believes that without some sort of legislation, the new Apple policy will result in serious crimes going unsolved.

The challenges to law enforcement to keep up with technological advances in this field are substantial. Digital device technology is changing at lightning speed, as is the technology to extract and analyze data from those devices. This poses serious problems for meeting requirements of *Daubert*—i.e., being able to demonstrate that digital evidence presented in court is reliable. It also poses problems for police agencies that must frequently purchase new technology to extract and analyze digital evidence and send staff for frequent training in how to use new technology. These kinds of purchases are often harder sells to mayors and city councils than the addition of officers, cars, or other more visible and easily understood investments.

The primary focus on digital evidence today is cell phones, though the practical scope is far wider than one category of device.

Digital evidence processing is a growing topic with increasing significance for investigations.

Clearly, digital evidence processing is a developing field with numerous potential needs to help realize its full potential for the criminal justice system. The following sections describe the workshop, which sought to identify and prioritize needs in this growing field.

WORKSHOP ON DIGITAL EVIDENCE NEEDS

In July 2014, RAND and the Police Executive Research Forum (PERF) held an NIJ-funded workshop with the purpose of examining challenges associated with digital evidence for the criminal justice community and identifying needs associated with digital evidence collection, management, analysis, and use. The workshop was intended to go beyond simply identifying technology needs to defining priorities among the potential technology solutions to those needs. There was a review of the current information on "demand" in this area (i.e., synthesis of current information on needs) as a precursor to discussing current "supply" (i.e., technologies that are available to meet the needs now and any available information on their data and utility). To define the scope for the workshop, a preliminary list of digital evidence challenges were identified. They were

- **exploitation and analysis of suspects' hardware devices,** such as computers, cell phones, GPS devices, or credit card fraud devices
- **collection and analysis of information related to crime or suspects in other IT systems,** such as social media, cloud storage systems, or private CCTV installations
- **search and analysis of websites,** including child pornography and human-trafficking sites, chat rooms, bulletin boards, or file-sharing networks.

The discussion was informed by considerations of how digital evidence is used in the courtroom, including chain-of-custody issues, handling of exculpatory evidence, and recent court decisions. The 24 participants in the workshop included 11 police digital forensic experts, two prosecuting attorneys, one privacy advocate, two industry representatives, two NIJ officials, and six project staff. The first half of the workshop included a brief discussion on digital evidence literature by PERF staff; a discussion of the process of obtaining, processing, and managing digital evidence; and a discussion of search-and-seizure, chain-of-custody, discovery, and other issues pertaining to the use of digital evidence in the courtroom. The second half of the workshop involved identifying specific technology needs related to digital evidence and criminal justice, as well as a Delphi exercise to identify priorities among those needs.

Digital evidence processing is a growing topic with increasing significance for investigations. One examiner at our workshop compared the state of digital forensics to "where DNA was twenty years ago, in terms of growth, how it is a new field in police forensics, and how with DNA people came up with great technologies" to address needs and make the best use of new evidence. Another examiner noted that digital evidence is "as important as firearms, fingerprints, DNA" and that "more cases are being solved on digital evidence than anything else right now."[8]

We provide here a general review of the workshop's discussion and the process to identify needs. In the next section, we will cover the prioritization of those needs via the Delphi process. In other words, we provide a qualitative review of the workshop and its outcomes followed by a quantitative analysis of the digital evidence needs.

Tactical Issues

The workshop started by reviewing general tactical issues regarding how law enforcement interacts with digital evidence. Given the diversity of attendees, we sought a shared understanding regarding what police do with digital evidence. From this understanding, we discussed common issues and needs among our participants. There were two main topics in this part of the workshop: managing an excess of evidence with minimal support; and training and staffing.

Excess of Evidence and Minimal Support

Law enforcement attendees were unanimous in noting the considerable quantity of evidence analyzed by examiners and

challenges in obtaining the necessary support. There are two interrelated issues with this topic, namely backlogs and command-level buy-in. Most agencies represented at our workshop reported a backlog in analyzing evidence, sometimes up to a year. One attendee said, "it gets to the point where I don't really like to take days off because I know when I come back my work has doubled." Contributing to the backlog is the lack of personnel trained in digital evidence extraction. Some of the representatives for larger agencies stated that only a handful of employees, both sworn and civilian, are dedicated for digital forensics. Additional challenges regarding backlogs are the constantly changing technology and required equipment for analysis. While those specific challenges will be addressed further in the context of training, we found that these challenges may have a self-reinforcing relationship with backlogs. This means the challenges affect backlogs, and then backlogs affect the challenges themselves within a feedback loop; a growing backlog prevents training opportunities because classes would take examiners out of the workplace, and a backlog can undermine requests to replace inadequate, antiquated, or underfunded technology and licenses due to budget constraints of units perceived to be performing slowly. The later difficulty directly relates to the issue of command-level support.

While cell phone analysis is a growing area of digital evidence processing, participants noted that they likely deal with as much video evidence—particularly from surveillance cameras—as they do cell phones. That said, there are limited tools available to reliably enhance and analyze video. In many cases with video, attendees note that what you see may be all you can get. An added challenge relates to the various codexes, or format of compressed data. Video may be unusable without the proper codex in place, like trying to open a computer file with an unknown extension. However, video is still an important tool and examiners are asked to find what they can with limited enhancement techniques, which thereby contributes to the backlog with limited positive results.

Given the excess of data, examiners stressed the importance of triaging digital evidence. Certain items and types of evidence within items (e.g., texts, email, GPS) must be placed at higher priority based on expected outcomes. Participants stressed that little has been done to develop software to aid in triage for examiners, though recent attempts have promise. An effective triage tool could assist nonexaminers in doing some preliminary analysis and could reduce the general workload of the forensic lab.

Law enforcement attendees repeatedly mentioned the challenge of getting their superiors to see the cost-effectiveness of digital evidence processing. One critical issue is the high cost of doing digital forensics. Attendees noted that providing necessary equipment, renewing licenses, and providing training can easily be in the tens of thousands of dollars; such cost is independent of the man-hour and personnel costs of those assigned to the digital unit. In fact, all attendees referenced the importance of federal/state funding sources and training, as local departments tend to keep the budgets of digital forensics units minimal.

Some workshop participants believe there is an inherent resistance to digital evidence by "old-timers who are not technical" and that many command staff "often live in an analog age where digital evidence wasn't really associated to a certain level of policing experience. . . . They don't understand the value and that it applies to policing in the 21st century." Others brought up another perspective on limited support by command staff: politics. Police chiefs need to work with elected politicians, and it may be easier to justify a budget to add beat officers or anti-violence programs rather than "having this extra person in this lab, which—especially after Snowden—isn't as politically feasible."

However, this challenge of upper-level support was not viewed as insurmountable by some attendees. Participants noted that chiefs and other police executives, while not very knowledgeable about specific technologies, did appreciate results of digital evidence processing and seeing results opened the door for more support. One digital evidence examiner mentioned that while "senior management probably isn't technical . . . they don't really care about it," opinions changed and resistance was easier to overcome once "we started winning cases and started showcasing results." Another described how his command staff first believed digital forensics to be a waste of manpower, but changed their

While cell phone analysis is a growing area of digital evidence processing, participants noted that they likely deal with as much video evidence.

Law enforcement attendees generally regarded assistance from both federal and state governments as critical to success in digital evidence processing.

perspective as the number of digital analysis requests doubled each year of the unit's existence.

Staffing and Training

Our next general topic covered the required staffing and training arrangements needed for effective digital evidence processing. Given that the field is still relatively new to policing, no meaningful standardization or best practices have been developed. The three major areas of our discussion were promotions, the role of government assistance, and the importance of teaching digital evidence within departments.

Promotions are a difficult conundrum for sworn members working in digital evidence units. While many officers seek to rise in rank, those working in digital evidence tend to cap their advancement. When a unit is small, there is limited need for multiple supervisors and, as one examiner put it, those promoted "will be back out on the street within minutes." This can harm the unit's functionality as well as discourage officer development. With the high costs of training, both monetarily and through experience, taking such officers off of digital evidence and back to patrol or command may not be efficient. One participant reported that the problem has "stopped me from taking the promotional exam because I am not willing to leave the unit."

While one potential solution to promotional issues is to hire more civilians for the highly technical digital evidence roles, this also has challenges. Participants generally believed that hiring civilians would not provide a clear net benefit. Civilian employees generally lack a clear route for promotion, though options are more limited given that civilians hired for digital forensics do not have ready alternate placement outside the unit like sworn personnel. Some examiners mentioned that civilians may have greater computer skills but have considerably less experience discerning which evidence is necessary and useful for investigations. While civilians may cost the departments less in the long run, some attendees noted that this structure gives civilians less incentive to stay for the long term when better-paying private-sector positions are available requiring the same skill set. If a civilian leaves the department, any training cost provided must be repeated with a new employee, which presents the same problem facing units following sworn promotions.

Law enforcement attendees generally regarded assistance from both federal and state governments as critical to success in digital evidence processing. The benefit of this assistance came up throughout the workshop in numerous contexts. Participants described how federal grants made it possible to hire detectives and obtain necessary equipment, such as Cellebrite machines and licenses, which go beyond departmental budget allotments. While some attendees noted how small agencies could take particular advantage, given the more limited potential budgets compared with large agencies, even the participants from larger departments estimated that "95 percent of our equipment" comes from outside funding.

Government-sponsored training was another type of financial assistance provided to departments. The rapid changes in technology require constant updates and technical assistance for numerous job-related outcomes, such as being qualified as an expert in court. This training quickly depletes limited local budgets. In response, federal agencies such as the Secret Service have provided extensive training at no cost to departments. According to one examiner, without such classes, "half of us wouldn't be here," and thanks to the Secret Service, "in the last three years, my department hasn't paid for any of my training."

Another examiner cited the importance of white papers and other training-related documents, such as the work from NIST, that provide guidance on best practices and equipment validity. Some attendees referenced NIJ-funded projects to develop better digital evidence tools, such as programs to extract data from GPS units preinstalled in automobiles. Other participants even noted the workshop itself as a federally funded project to gather expert opinion and generate needs for future funding opportunities that would not have been feasible otherwise.

Participants not working in law enforcement echoed the importance of government training. One prosecutor noted being invited to attend multiple government-sponsored events and learning a great deal about digital evidence. Sessions held

by the Secret Service are open to civilian as well as sworn members of digital evidence task forces.

However, some participants cautioned against too much reliance on outside funding. While the financial assistance can help procure one-time or infrequent purchases, much of the cost in digital forensics comes from repeated purchases (e.g., training, licenses) or annual budget items (e.g., personnel). Without regular assistance, departments reliant on this funding are faced with limited options, such as cutting back unit functionality or shifting budget resources to cover new recurring costs. One attendee offered that when jurisdictions "become dependent on federal grants" that eventually end, agencies become "stuck" once on their own. This pitfall is amplified when the command staff does not fully appreciate the value of digital forensics and does not provide sufficient resources to match demand. Given the growing role and importance of digital evidence, drastic cuts may prove counterproductive to investigations.

The popularity of and reliance on government assistance for various training opportunities also affects the final area within the staffing and training topic, namely the importance to teach digital evidence processing at all levels. While there was clear support for continued training within digital forensic units, participants strongly believed in the need to train all levels of staff, including patrol officers, detectives, and police executives.

Many attendees suggested that police academies should expand their digital evidence curriculum beyond the introductory level. As one examiner noted, "we have training that everybody has to go through [periodically] and you get first aid, CPR, and all that stuff, but when we start to talk about digital evidence, [the response is] we don't have time for that . . . but the digital evidence issue is going to start costing us if we don't address it." Greater coverage of digital evidence processing could increase efficiency, improve evidence preservation, and manage expectations. Many examiners complained of receiving excess requests to extract data from devices, due in part to lack of investigative training of patrol officers and detectives. One examiner likened the situation to asking the fingerprints unit to dust an entire warehouse where a small crime scene exists just to ensure "everything" is obtained, even if most is irrelevant. Training can lead to a level of discernment by those directly investigating cases. Also, training can improve the preservation of evidence, such as educating patrol officers on the necessity of a Faraday bag to isolate electronic devices—especially in light of the *Riley* decision, where most searches of a device will require a warrant. Finally, training can help to manage expectations of those who rely on digital evidence examiners for what can be obtained and how quickly it can be obtained. Numerous participants lamented that other officers or even prosecutors underestimated the quantity of data and the time necessary for analysis.

Attendees also discussed the potential to give basic digital evidence tasks to patrol and detectives. This process could give others an insight into what type of evidence to collect and aid in reducing backlogs for digital examiners. Some agencies have already started implementation of such efforts for case detectives. One participant described how detectives could use a designated computer to provide a basic logical extraction before submitting a device for a subsequent, more detailed analysis by digital examiners. There was some concern whether such actions would provide difficulties at trial, as the detective is not considered an expert and could not necessarily testify to the methods used for data extraction. However, multiple attendees noted that the basic analysis would only serve as a starting point for investigation and would be confirmed by expert examiners; the purpose of giving nonexaminers the ability to obtain some digital evidence safely is to move investigations forward and not have time-sensitive investigative leads held up by backlogged digital evidence units.

As previously noted, many participants expressed frustration at a command staff that seems to remain in the "analog age." It was no surprise to hear discussion regarding the need for digital education among the higher echelon. While participants noted that command gained insight from closures through digital evidence, they also reiterated the desire to have greater buy-in for funding and support. However, some attendees expressed skepticism at the degree of support police executives could give after considering the political issues involved, such as reallocating money to fund more street officers or funding programs seen as similar to the recent NSA data privacy scandals.

However, some participants cautioned against too much reliance on outside funding.

Judges, juries, and defense attorneys also have a stake in digital evidence processing.

Legal and Courtroom Issues

The next major segment of the workshop examined legal and courtroom considerations for digital evidence. The role of law enforcement does not end with an arrest or clearance. Police must give evidence to prosecutors and effectively communicate both the process of obtaining digital evidence and its significance to all parties, including a jury. Due to the exclusionary rule, even the most convincing digital evidence may never be part of the court case if the device was seized or searched illegally. Mutual understanding and shared expectations between law enforcement and prosecutors are necessary to provide justice and increase perceptions of legitimacy for the criminal justice system. The workshop covered three main areas within this segment: case coordination between law enforcement and prosecutors, the impact of digital evidence on other courtroom actors, and methods to make digital evidence cases stronger.

Case Coordination with Prosecutors

While police build a case through investigation, detectives must be cognizant of courtroom requirements. The primary law enforcement partner within the court is the prosecutor, as both serve as the government's representatives within the criminal justice system. While this results in a close alignment of interests, there are some challenges that necessitate additional coordination between the parties. First, prosecutors may lack knowledge regarding digital evidence, and second, prosecutors must address privacy-based legal objections to digital evidence.

Both law enforcement and courtroom participants in our workshop noted potential difficulties with prosecutors not understanding elements of digital evidence. This lack of knowledge is similar to challenges faced on the law enforcement side where detectives underestimate the quantity and time frames involved in digital analysis. One examiner remarked that, "our prosecutors don't even look at the evidence until the trial," while another examiner mentioned that prosecutors ask for everything and "then a day before . . . they take a look at it and say, 'Why do I need all this?'" In response, an attendee who serves as a prosecutor mentioned that it is necessary to meet with digital examiners early in the process of case preparation and understand that search parameters must be narrowed ahead of time.

A balance must be struck between data and privacy considerations that prosecutors must address while compiling and entering evidence. Participants agreed that the arguments for case efficiency and maintaining legal privacy closely aligned in this situation. One attorney noted that, since only some data on a device is relevant to a case, coordination between police and prosecutors increases efficiency and reduces the workload of digital evidence examiners. Additionally, law enforcement participants acknowledged no interest in legally overstepping their boundaries for digital searches—any actions that open agencies to legal liability can result is further reductions of staff or equipment, so "we are actually a lot more cautious than one may imagine." As another examiner put it, "we don't want abuses because then things get taken away from us."

Impact on Other Courtroom Actors

Judges, juries, and defense attorneys also have a stake in digital evidence processing. Attendees noted that judges rarely sustain objections to the introduction of digital evidence as long as the evidence meets the *Daubert* standard. As for juries, one prosecutor remarked, "they love it, they eat it up." While judges and juries are apparently receptive to digital evidence, participants agreed that defense attorneys are far behind in understanding and challenging digital evidence. One examiner who has testified on digital evidence reported, "defense attorneys tiptoe around me and they are careful not to ask me something they don't know about, but they know less than the patrol officers." One reason that defense attorneys may be behind is because they receive evidence through discovery weeks after the prosecutors do and therefore have even less time to sift through the amount of information. While defense attorneys can challenge how the records were acquired and chain-of-custody issues, especially in the context of the cloud, most are ineffective at pushing back against digital evidence presented by the prosecution. All participants, though, predict that defense attorneys will eventually obtain a parity of digital evidence knowledge that will result in more successful challenges.

Making Cases Stronger

As digital evidence plays a larger role in cases and as defense attorneys develop strategies to rigorously question findings, there is a clear prosecution interest to increase the credibility and validity of digital information introduced as evidence. Participants discussed a number of techniques that would assist in improving the strength of cases involving digital evidence, including validating software, meeting the *Daubert* standard, and obtaining comprehensive search warrants.

Numerous participants mentioned the importance of having validated tools for digital evidence detection and extraction. One workshop participant noted potential problems from nonvalidated tools or processes in reference to the Casey Anthony murder trial in Florida during 2011—in that case, investigators did not fully capture Internet browsing history data from the family's computers, and therefore missed searches relevant to the case (see also, Casey Anthony detectives overlooked Google search, 2012). Another attendee remarked that continued training and validation are important for digital examiners to maintain their status of experts during testimony. One participant expressed appreciation that agencies can rely on white papers by governmental organizations to guide them toward validated tools.

As technology continues to develop rapidly, training and equipment used by digital evidence examiners will rapidly become obsolete, raising fears that future applications of the *Daubert* standard may keep evidence out of court. For example, one participant described a new extraction technique where general benchmarks existed but had not been peer reviewed. When questioned how this would satisfy *Daubert*, another attendee noted that the general process would qualify if it is considered an update to known procedures. Still, efforts are necessary to ensure digital evidence meets the *Daubert* standard moving forward, and that such efforts can face critical scrutiny, even if they may not have thus far, as defense attorneys become more knowledgeable.

Finally, cases are made stronger through comprehensive use of search warrants. Using warrants helps to preclude evidence from being ruled as inadmissible. Surprisingly, participants did not see the *Riley* decision as a major change, if only because most in attendance already held a strict policy to always obtain a warrant for a search. Of course there are Fourth Amendment exceptions for exigent circumstances, which were also acknowledged and confirmed in *Riley*, but the general encouragement is to obtain a warrant. Participants viewed the warrant process as easy to complete within their investigations, and one attendee noted surprise at how "digital evidence language has popped up in boiler plate search warrants." Still, there are challenges in the warrant process. One example is when evidence outside the warrant is found during a search, such as finding child pornography during a fraud case. In that scenario, attendees agreed that analysis must come to a full stop until an additional warrant is obtained. Another example involves digital evidence on servers outside of the agency's location, particularly in another country. Many participants voiced frustration at the international protocols necessary to obtain digital evidence outside national borders. One attendee described how it took nearly two years to receive digital evidence through an MLAT. However, all agreed that investigators must follow the process lest any obtained evidence be tainted in court.

Identifying Specific Needs to Improve Digital Evidence Utilization in Criminal Justice

Following these discussions, the panel and research team identified a list of needs connected to digital evidence processing. Drawing on the results of the literature review by project staff, the panel engaged in a structured brainstorming process to identify specific needs that—if met—would improve the utilization of digital evidence in the criminal justice system. The problems and challenges discussed in this section were the foundation for needs generation. Needs directly related to the points raised (e.g., development of training materials to remedy training shortfalls identified by the panel) were identified in each of the critical areas of discussion regarding law enforcement issues (such as evidence collection, staffing, and executive support), in addition to legal and courtroom issues that affect the final disposition of cases involving digital evidence. Additional brainstorming identified other needs to fill out the picture of law enforcement, corrections, and courts needs related

Numerous participants mentioned the importance of having validated tools for digital evidence detection and extraction.

The discussions of the panel identified 34 different needs that, if filled, could improve the capabilities of the criminal justice system with respect to digital evidence.

to digital evidence. In the next section, we present the full list of needs and the results of their prioritization.

PRIORITIZING DIGITAL EVIDENCE NEEDS

The discussions of the panel identified 34 different needs that, if filled, could improve the capabilities of the criminal justice system with respect to digital evidence. For different parts of the "innovation system"—including government research funders, criminal justice agencies, technology developers, technical assistance providers, and so on—such a broad listing of potential targets for effort and investment is useful. However, for developing a more focused set of innovation targets and helping to enable trade-offs where choices among different possible investments must be made, prioritization is needed. As a result, after generating the potential needs with the participants in the workshop, we drew on their expertise to rank the different ideas on a number of different factors to identify which rose to the top as potentially most valuable or attractive.

The Logic of Rating the Digital Evidence Needs

The needs were prioritized using a variation of the Delphi method,[9] a technique developed at RAND to elicit expert opinion about well-defined questions in a systematic and structured way. In this case, the logic of the rating process was as follows:

1. how each of the needs was viewed as benefiting different—though admittedly complementary—objectives related to improving digital evidence capabilities and utilization:
   - acquiring digital evidence more effectively
   - analyzing it more effectively
   - searching and organizing it more effectively
   - reducing the man-hours required to analyze it and reducing digital forensics backlogs
   - facilitating chain of custody and authentication of digital evidence (i.e., bolstering its utility in court)

   All of the needs identified by the participants were viewed as contributing across all five categories, though doing so to differing extents. Each participant rated each need on a scale of 1 to 9 for each category (where 1 corresponded to contributing nothing to the objective and 9 indicated that meeting the need could result in a 20-percent or greater improvement in performance).
2. how technically difficult the participants believed it would be to meet the need—while meeting some needs might require only minor adaptation of an existing technology, others might be very technologically difficult. The participants rated each need's chance of technical success on a scale of 1 (10-percent chance of succeeding) to 9 (90-percent chance of succeeding).
3. whether criminal justice organizations would actually use the solution or technology if it became available—e.g., the greatest innovation might not be used if it was too expensive or incompatible with important organizational policies, while other innovations might be rapidly picked up. The participants rated each need's chance of operational success on a scale of 1 (10-percent chance of being broadly adopted and used) to 9 (90-percent chance).

These three scales sought to capture the key components that are needed to calculate the expected value of a possible innovation—how valuable it would be multiplied by the probability it could be successfully produced and, if produced, would be used. Rather than simply asking a group of experts to rank a set of options and taking the average of many responses, the Delphi method seeks to identify and explore differences among experts' responses. As a result, ratings are done in multiple rounds, with discussions in between focusing on specific ratings where there were divergences among the group. For this effort, two rating rounds on the needs were done with one intervening discussion, with the discussion spending the most time on cases where there was a great deal of spread in the responses

across the groups. The Delphi process used in this work builds on previous RAND work examining criminal justice technology, police, and practice needs (Hollywood et al., 2015; Jackson et al., 2015). Additional detail on the ranking methods and outcomes is included in the online appendix to this paper.

The Prioritized Digital Evidence Needs

The effectiveness of expert elicitation processes like the Delphi method relies on the knowledge and capabilities brought to the process by the participants. In identifying and selecting workshop participants, we sought to build a panel with a mix of perspectives and views, though within the context of an effort focused on digital evidence needs related to law enforcement organizations. As a result, the majority of the panel came from law enforcement, but additional participants from courts, the private sector, and civil society groups contributed their perspectives to needs identification and ranking, as well. All the workshop attendees, except the project and NIJ staff, participated in the ranking process.

We took each of the scores assigned by each participant and calculated an expected value for each need—multiplying together the benefit scores for each objective with the probabilities of technical and operational success. All the objectives were rated equally, e.g., acquiring digital evidence more effectively was viewed as equally valuable as reducing the man-hours required to process it. To rate each need, we used two calculations. First, and primarily, we took the median expected value that was assigned by the participants—which provides reasonable estimates of the center of the data even if there are outliers in the rankings. Second, we took averages of the expected values and identified needs that were not top-ranked by medians but had high average rankings. Given the variety of participants in the panel, these high-average expected-value needs were viewed as potentially reflecting needs that were viewed as very valuable by particular participants and therefore valuable to include in the top tier. Three additional needs were identified via this method. This resulted in a top-tier list of nine of the 34 identified needs. The online appendix to this document presents a detailed discussion of the rating methods and individual need rankings.

Key among the nine top-tier needs were educating prosecutors to make more-focused use of digital evidence and of judges to enable its use in court, enabling first-responding officers to be better prepared for incident scenes where digital evidence might be present, providing better prioritization and triage analysis of digital evidence given scarce resources, developing regional models to make digital evidence analysis capability available to small departments, acquiring new tools for collection and analysis of digital evidence, and addressing concerns about maintaining the currency of training and technology available to digital forensic examiners. The remaining needs ranged from approaches to addressing organizational concerns limiting law enforcement capability in digital evidence (e.g., promotion and management concerns) to specific technical issues in collecting and processing specific types of evidence. The top-tier digital evidence–related needs identified by the participants are included in Table 1. The remaining, lower-tier needs are presented in Table 2.

Looking across the needs identified to better utilize digital evidence, all were viewed as contributing—at least to some extent—to each of the five areas identified (acquiring; analyzing; searching and organizing evidence; saving time or reducing backlogs; or facilitating chain of custody and authentication). The lowest average ranking across the participants for any need was 3 (i.e., only just making it into the lower third of the ranking scale). The technical feasibility of the needs were viewed as relatively high, with the lowest average technical feasibility ranking for any need above 5 (the middle of the scale). Rankings for operational feasibility (i.e., the likelihood that solutions to the need would be broadly used) were lower overall, with averages ranging from just over 3.5 for the lowest-rated need to a high of just over 7. The relatively narrow spread in both the rankings of technical and operational feasibility meant that overall rankings were driven by the perceived benefits of meeting the different needs, particularly the number of the objectives for which the need was ranked particularly high.

Table 1: Top-Tier Digital Evidence Needs

Problem or Opportunity	Associated Needs
Prosecutors have a tendency to request all information off devices without considering the challenge posed by large volumes of data.	• Expand available federal-level training at existing training schools to build knowledge across system.
First-responding officers to an incident or arrest often do not know how to secure and use digital evidence to preserve chain of custody and later admissibility in court; e.g., "a detective searching a computer on his own."	• Integrate digital evidence practices into academy training—at least at the awareness/basic training level.
Departments do not have enough personnel to process volume of digital evidence, no matter what tools are used, resulting in large backlogs.	• Develop better prioritization or triaging methods or tools for cases and for what evidence to extract within cases (either for digital evidence examiners or potentially tools usable by officers in the field).
Smaller departments lack capacity to address digital evidence.	• Develop regional models for building capability where small departments pay to fund common resources. Incentives could be created through grant mechanisms to facilitate this approach.
The acceptability of results of digital evidence analysis can be challenged in court when extraction and analysis is not performed with the most up-to-date tools.	• Routinely update the training and tools available to examiners to ensure they are using the current technology.
Lack of knowledge about digital evidence on the part of judges complicates appropriate use in court.	• Expand available federal-level training at existing training schools to build knowledge across system.
Departments lack tools to represent complex data sets in understandable ways for investigation and presentation.	• Utilize existing software tools for analysis of data sets like cell tower data. Examples exist that are web-based and can be bought on a case-by-case basis, but knowledge of what is available is limited.
Volume of data coming from closed-circuit television (CCTV) cameras and video is a challenge—and there are limited tools for evaluating and processing evidence.	• Departments must acquire in-house tools to process video evidence.
Collecting digital evidence from victim devices—where broad capture of all data on phone might capture data law enforcement "doesn't want" (e.g., sexting materials)—can be problematic.	• Develop tools that allow more narrow collection of data from devices to respect victim privacy while still meeting investigative or protective needs.

Table 2: Lower-Tier Digital Evidence Needs

Problem or Opportunity	Associated Needs
Departments do not have enough personnel to process volume of digital evidence, no matter what tools are used, resulting in large backlogs.	• Increase sworn-in manpower devoted to digital forensics activities. • Define roles for lower-paid "digital evidence assistants" who can perform routine examinations. • Address pay scale issues to make it possible to successfully recruit civilian staff for technical roles.
Some GPS devices available on the market use proprietary software and access technologies that make it difficult to extract data during investigations.	• Utilize alternative approaches to acquire data from the company (e.g., execute search warrants on companies for data that these devices transmit to company servers) rather than focusing on the devices themselves.
Encryption and passwords on mobile phones prevent access.	• Develop alternative access methods to address encryption.
It can be difficult to access on-car digital evidence from systems such as OnStar (and other devices that cannot be removed from the platforms).	• Develop tools to allow easier access to that data without disassembling/destroying devices, while also maintaining chain of custody.
Managing multiple video evidence streams (e.g., business CCTV, personal cell phone video) during large incidents poses a data management and analysis challenge.	• Develop information systems to better manage data, link with metadata, etc. to allow searchability and analysis.
Having to pay for access to historical data sets of public data (e.g., Craigslist posts) poses a cost challenge for departments.	• Build a public access data set for law enforcement for investigative purposes that captures and archives such data.
The performance and acceptability of new evidence collection and analysis techniques for criminal justice use are uncertain.	• Provide timely validation/evaluation of technologies and analysis types of different products and techniques against established standards.
Departments face real difficulty in maintaining capability to collect and analyze digital evidence given the pace of technological change.	• Develop more standardized certifications for digital forensics personnel, including continuing education requirements.
Need ways to collect "routine" digital evidence in a way that does not require full examiner involvement, and does not always require seizure of the device (e.g., from a crime victim).	• Develop deployable tools for detectives to collect evidence in the field, but design in such a way that addresses potential for misuse and appropriately controls information and access.
Current tools for explicit image detection are not effective at identifying explicit images.	• Enhance explicit image detection to narrow how many images need to be reviewed by examiners.
The practice of "promoting out" staff from digital evidence units pose a problem for agencies to maintain technical proficiency.	• Create a promotion track within specialist units.
Investigators may have no way to identify that data in suspect or victim cloud storage accounts exist and could provide investigative leads.	• Develop tools to identify where accounts exist to trigger follow-up investigation.
Some courts are skeptical of digital evidence due to uncertainties about chain of custody and validity of information obtained from devices.	• Need an effort to systematically validate the performance of digital evidence tools to ensure they can withstand *Daubert* challenge.
Law enforcement lacks tools to analyze some types of electronic systems and devices.	• Develop digital evidence tools to examine gaming devices. • Develop digital evidence tools for examining networks. • Develop digital evidence tools for examining routers.
Proprietary codexes for video evidence can create analysis problems.	• Though commercially available video conversion tools allow conversion through screen capture, improvements that reduce the time required for such conversion would be valuable.

Table 2—Continued

Problem or Opportunity	Associated Needs
Technologies developed to address problems have a "whack-a-mole" character trying to catch up with innovation.	• Consider prize models to create incentives for many different private-sector actors to work on different digital evidence problems simultaneously.
Cross-international-border issues create significant challenges for issuing and serving warrants for electronic information from entities in other countries.	• Improve efficiency of MLAT processes for requesting information from foreign entities.
Agency budget constraints make it difficult to maintain the currency of digital evidence tools and software packages.	• Develop low-cost or free digital evidence analysis tools.
Virtual currencies pose challenges for investigations.	• Develop tools to identify presence of virtual currency on seized devices.
Within agencies, a lack of leadership commitment to sufficiently funding digital evidence analysis capacity limits the ability to build and maintain expertise.	• Develop information to make the case for building and maintaining digital evidence analysis capability outside of federal grant streams, preparing departments for making the transition to funding these capabilities internally.
Quality of video evidence can limit use of other analytic tools (e.g., facial recognition).	• Develop information to help persuade entities to adopt better video technologies to broaden technology options for analysis.

CONCLUSIONS—FOSTERING INNOVATION IN DIGITAL EVIDENCE

The field of digital evidence is new and rapidly expanding. Potentially, digital evidence offers an important new source of information that will help prosecutors win more convictions. Using GPS data to place suspects at or near the scene of a crime, analyzing text messages and email to corroborate charges, capturing incriminating photos from social media sites, and gathering information on criminal associates from cell phone address books or social media metadata are just a few of the ways in which electronic data provides police and prosecutors with a source of information heretofore unavailable. As the types and sophistication of electronic media from which digital evidence can be gleaned increase, this type of evidence will become an essential part of investigating and prosecuting most crimes.

However, while the potential is great, there are significant challenges in exploiting digital evidence. We heard in the workshop that departments are still playing catch-up: Command-level staff often does not appreciate the workloads of digital evidence examiners and fails to allocate personnel resources sufficient to keep up with growing demand. Obtaining additional funds for this function from city councils is a harder sell than asking for more cops on the street, although the need is acute and the potential payoffs substantial. Work backlogs are exacerbated by lack of training among patrol officers and detectives about which devices are important to confiscate in different types of cases—the result being that they often grab everything available without thought of relevancy. Moreover, the departments that we heard from in the workshop were all large and among the most technologically sophisticated in the country: The need and the challenges are almost certainly greater in medium-sized and small agencies.

Another set of challenges to the effective use of digital evidence arises from civil liberty concerns. Courts are placing more restrictions on the ability of law enforcement to seize devices and narrowing the scope of what information may be retrieved. This trend is most recently embodied in the *Riley* decision, which, for the first time, ascribes a special evidentiary status to information contained in portable electronic devices. The recent announcements by both Apple and Google that would make data on cell phones virtually unavailable to law enforcement even with a search warrant may prove to be a significant impediment to accessing digital evidence without voluntary authorization of the device owner. However, digital evidence is not just resident on phones and devices, but captured by the networks these devices connect to—meaning that effective use means understanding not just the importance of the devices themselves, but what information is captured where via their use. This is a rapidly changing landscape that police agencies and prosecutors need to keep up with and respond to.

Top-tier needs identified through the workshop Delphi process closely agreed with prioritization of needs gleaned from reviewing workshop notes. Key among those needs were

These top-tier needs highlight a path for innovation, through funding and training at all levels of the criminal justice system, that can allow digital evidence to reach its full potential for law enforcement and courts.

- *Educate prosecutors to make more-focused use of digital evidence.* Many prosecutors do not yet have a good understanding of the uses and limitations of digital evidence in the courtroom. Consequently, they request that more information be extracted from devices than necessary, creating needless work for digital evidence examiners. Expansion of federal training programs to include more prosecuting attorneys would give them a greater understanding of what data are necessary for evidence in different types of cases.
- *Educate judges to better understand the issues surrounding use of digital evidence in the courtroom.* Some judges lack knowledge about processing and extraction techniques regarding digital evidence. Expanding federal training programs to include judges would help give them a better foundation in issues surrounding this type of evidence.
- *Enable first-responding patrol officers and detectives to be better prepared for incident scenes where digital evidence might be present.* First-responding officers to an incident or arrest often do not know how to secure and use digital evidence to preserve chain of custody and later admissibility in court. Training on digital evidence handling and preservation at the academy level and as a part of investigator training would promote better evidence preservation and limit seizing of devices not relevant to an investigation.
- *Provide better prioritization and triage analysis of digital evidence given scarce resources.* Departments do not have enough personnel to process the volume of digital evidence, resulting in large backlogs. This situation would be helped by providing tools for detectives in the field to triage evidence and developing guidelines for digital evidence examiners to better prioritize their workload.
- *Develop regional models to make digital evidence analysis capability available to small departments.* Small agencies, in particular, lack resources for effective collection and analysis of digital evidence. Partnerships with larger departments in the area could provide common resources available across regional agencies.
- *Address concerns about maintaining the currency of training and technology available to digital forensic examiners.* Digital devices and extraction tools change rapidly. Examiners need new tools and frequent training on new technologies to keep current with the field.

These top-tier needs highlight a path for innovation, through funding and training at all levels of the criminal justice system, that can allow digital evidence to reach its full potential for law enforcement and courts.

Notes

[1] This working definition from NIJ is not exclusive to digital evidence, in that the analysis of physical data (such as DNA or fingerprints) could technically meet the definition as computers are used to process physical items. However, digital evidence is exclusive to this definition in that any evidence not meeting the criteria is not considered digital evidence. Additionally, digital evidence cannot exist without an electronic device, whereas analyzed physical evidence is aided by but does not require electronics.

[2] While both are advanced techniques, there are technical differences between the two options. Chip-off is when the memory of a device is manually removed for analysis, which requires "extensive training in electronic engineering and file system forensics" (NIST, 2013). Micro read techniques examine memory using a microscope to read the physical gates (whether open or closed) and then convert results into binary and ASCII. Such techniques are very time-consuming and are rarely used, but would be a good option if the memory chip had been extensively damaged.

[3] While acts of brute force can damage data, numerous digital processes such as accessing apps or connecting to different remote towers/networks can also alter data, whether intentionally or not. Law enforcement is trained to deal with physical preservation, but digital preservation is a new arena. Toward this end, the use of Faraday bags are suggested as a preservation tool to prevent devices from sending or receiving signals.

[4] It is important to appreciate that law enforcement does not work in a vacuum and often needs to be acutely aware of legal issues. In cases of digital evidence, given the privacy concerns, data collected by police without admissibility in mind will likely result in far greater problems than potential benefits in determining new leads. This balance is in contrast to evidence that may not be admissible, such as a polygraph, but can provide new avenues for investigation—the polygraph is not useful in court but also does not undercut the fruit of related investigation as improperly searched/seized digital evidence can, as seen in the *Riley* decision.

[5] Note that state laws and judicial doctrine vary with respect to the plain view exception. A full exposition of individual state requirements are beyond the scope of this paper.

[6] See also *United States v Henderson* (2014) (testimony about which towers a suspect connected to was ruled not to be expert testimony).

[7] In a subsequent post, Kerr (2014c) notes that, while Apple's policy may impede investigations, the "backdoor" that Apple had maintained presented security risks. In particular, it created an opportunity for hackers to break into iPhones remotely. In the second article, Kerr admits that it is hard to decide which is the greater of the two potential problems.

[8] Undoubtedly, police use digital evidence extensively given the ubiquity and storage capacity of digital devices. This use is not limited to digital-related cases or "cybercrime," as the examples in our introduction clearly demonstrate. However, there has been no systematic, empirical examination regarding the impact of digital evidence on case clearance. Such a study would be ambitious but possibly provide critical insight into the role of digital evidence in police investigations.

[9] The web reference to the Delphi method (RAND Corporation, undated) includes the formative RAND papers on the method and more-recent applications of the technique to a range of policy problems.

References

Alvarez, L. (2011, July 18). Software designer reports error in Anthony trial. *New York Times*, p. A14.

Annual wireless industry survey. (2014, June). *CTIA.* As of September 25, 2014:
http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey

Brady v Maryland, 373 U.S. 83 (1963).

Burch, A. D. S. (2014, September 12). Pedro Bravo found guilty of first-degree murder of Christian Aguilar. *Miami Herald* [online]. As of March 15, 2015:
http://www.miamiherald.com/news/local/community/miami-dade/article1980000.html

Casey Anthony detectives overlooked Google search for "fool-proof" suffocation methods, sheriff says. (2012, November 26). *CBS News* [online]. As of October 16, 2014:
http://www.cbsnews.com/news/casey-anthony-detectives-overlooked-google-search-for-fool-proof-suffocation-methods-sheriff-says/

Cusack, B., & Son, J. (2012, December). *Evidence examination tools for social networks.* Australian Digital Forensics. Conference. Perth, Western Australia.

Daubert v Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993).

Degani, M. (2014). *Recent court decisions: Electronic evidence.* U.S. Department of Justice, Computer Crime and Intellectual Property Section. Washington, DC.

Delport, W., Köhn, M., & Olivier, M. S. (2011). Isolating a cloud instance for a digital forensic investigation. In H. S. Venter, M. Coetzee, and M. Loock (Eds.), Proceedings of the 2011 *Information Security for South Africa (ISSA 2011) Conference.* Johannesburg, South Africa: ISSA.

Fakhoury, H. (undated). *Legal issues involving electronic evidence.* Unpublished paper commissioned by the Police Executive Research Forum, Washington, DC.

Electronic Frontier Foundation. (undated). *FAQ on the CALEA expansion by the FCC.* As of March 13, 2015:
https://www.eff.org/pages/calea-faq#1

Federal Rules of Evidence, Article VIII—Hearsay, 801(d)(2)—Statements that are not hearsay; an opposing party's statement.

Federal Rules of Evidence, 702—Testimony by expert witnesses.

Frye v United States, 54 App. D.C. 46, 293 F. 1013 (1923).

Giglio v United States, 405 U.S. 150 (1972).

Graham, W. R., Jr. (2000). Uncovering and eliminating child pornography rings on the Internet: Issues regarding and avenues facilitating law enforcement's access to Wonderland. *Law Review of Michigan State University-Detroit College of Law*, 457.

Hollywood, J. S., Boon, J. E., Jr., Silberglitt, R., Chow, B. G., & Jackson, B. A. (2015). *High-priority information technology needs for law enforcement*, Santa Monica, Calif., RAND Corporation, RR-737-NIJ. As of March 15, 2015:
http://www.rand.org/pubs/research_reports/RR737.html

Horton v California, 496 U.S. 128 (1990).

Jackson, B. A., Russo, J., Hollywood, J. S., Woods, D., Silberglitt, R., Drake, G. B., Shaffer, J. S., Zaydman, M., & Chow, B. G. (2015). *Fostering innovation in community and institutional corrections: Identifying high-priority technology and other needs for the U.S. corrections sector*, Santa Monica, Calif., RAND Corporation, RR-820-NIJ. As of March 15, 2015:
http://www.rand.org/pubs/research_reports/RR820.html

Kerr, O. (2014a, June 25). The significance of Riley. *Washington Post* [online]. As of June 26, 2014:
http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/25/the-significance-of-riley/

———. (2014b, September 19). Apple's dangerous game. *Washington Post* [online]. As of September 19, 2014:
http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game/

———, (2014c, September 22). Apple's dangerous game, part 2: The strongest counterargument. *Washington Post* [online]. As of March 23, 2015:
http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/22/apples-dangerous-game-part-2-the-strongest-counterargument/

Latonero, M. (2011). *Human trafficking online: The role of social networking sites and online classifieds*. Los Angeles: USC Annenberg School of Communication. Available at Social Science Research Network. As of March 15, 2015:
http://ssrn.com/abstract=2045851

Leyden, J. (2014, September 23). Apple slaps a passcode lock on iOS 8 devices, but cops still inhale your cloud. *The Register* [online]. As of September 23, 2014:
http://www.theregister.co.uk/2014/09/23/icloud_hole_in_ios8_passcode_protection/

Mislan, R. P., Casey, E., & Kessler, G. C. (2010). The growing need for on-scene triage of mobile devices. *Digital Investigation*, *6*, 112–124.

Morse, D. (2014, May 6). Philip Welsh's simple life hampers search for his killer. *Washington Post* [online]. As of March 15, 2015:
http://www.washingtonpost.com/local/crime/philip-welshs-simple-life-hampers-search-for-his-killer/2014/05/05/1fd20a52-cff7-11e3-a6b1-45c4dffb85a6_story.html

Murphy, J. P., & Esworthy, M. A. (2012). The ESI tsunami: A comprehensive discussion about electronically stored information in government investigations and criminal cases. *Criminal Justice*, *27*, 31.

Mutawa, N., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. *Digital Investigation*, *9*, S24–S33.

National Institute of Justice. (2007a). *Digital evidence in the courtroom: A guide for law enforcement and prosecutors.* U.S. Department of Justice, Washington, DC.

———. (2007b). *Investigative uses of technology: Devices, tools, and techniques.* U.S. Department of Justice, Washington, DC.

———. (2008). *Electronic crime scene investigation: A guide for first responders, second edition*. U.S. Department of Justice, Washington, DC.

National Institute of Standards and Technology. (2013). *Guidelines on mobile device forensics (draft),* special publication 800–101. U.S. Department of Commerce, Gaithersburg, MD.

———. (2014). *New forensic subcommittee on digital evidence added to organization of scientific area committees.* U.S. Department of Commerce, Gaithersburg, MD. As of September 15, 2014:
http://www.nist.gov/forensics/forensics-090814.cfm

NIJ—*See* National Institute of Justice.

NIST—*See* National Institute of Standards and Technology.

Pipitone, T. (2012). Cops, prosecutors botched Casey Anthony evidence. *Click Orlando* [online]. As of December 3, 2014:
http://www.clickorlando.com/news/Cops-prosecutors-botched-Casey-Anthony-evidence/17495808

RAND Corporation. (Undated). *Delphi Method*. As of March 27, 2015:
http://www.rand.org/topics/delphi-method.html

Riley v California, 573 U.S.___ (2014).

Ruan, K. (2011, June 3). *Cloud forensics: An overview.* Cloud Futures 2011: Microsoft Research. Redmond, WA.

United States v Comprehensive Drug Testing, Inc. 579 f.3d 989; 9th Cir. (2009).

United States v Evans, 892 F.Supp.2d 949 N.D.Ill. (2012).

United States v Henderson, 564 Fed.Appx. 352 10th Cir. (2014)

United States v Stirling, No. 1:11-cr-20792-CMA, at p. 5 S.D. Fla. (2012).

United States v Williams, 592 F3.d 511, 515-17; 4th Cir. (2010).

United States v Wurie, 728 F.3d 1, 1st Cir. (2013).

U.S. Code, Title 18, Crimes and Criminal Procedures, Part I, Crimes, Chapter 119, Wire and Electronic Communications Interception and Interception of Oral Communications. As of March 24, 2015:
http://www.gpo.gov/fdsys/granule/USCODE-2011-title18/USCODE-2011-title18-partI-chap119-sec2510/content-detail.html

U.S. Code, Title 18, Crimes and Criminal Procedures, Part I, Crimes, Chapter 121, Stored Wire and Electronic Communications and Transactional Records Access. As of March 24, 2015:
http://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/html/USCODE-2010-title18-partI-chap121.htm

U.S. Code, Title 18, Crimes and Criminal Procedures, Part I, Crimes, Chapter 206, Pen Registers and Trap and Trace Devices. As of March 24, 2015:
https://www.law.cornell.edu/uscode/text/18/part-II/chapter-206

U.S. Code, Title 42, Public Health and Welfare, Chapter 21A, Privacy Protection. As of March 24, 2015:
https://www.law.cornell.edu/uscode/text/42/chapter-21A

Zawoad, S., & Hasan, R. (2013). Digital forensics in the cloud. *CrossTalk. The Journal of Defense Software Engineering, 26*(5), 17–20.

Acknowledgments

The authors would like to acknowledge the participation and assistance of Dulani Woods at RAND and Nathan Ballard at PERF during the Digital Evidence workshop. In addition, we were informed by analysis carried out by Hanni Fakhoury in the context of ongoing work with PERF and RAND for the Bureau of Justice Assistance. We would also like to acknowledge the contributions of Martin Novak and Steve Schuetz of the National Institute of Justice. The authors also acknowledge the valuable contributions of the two peer reviewers of the document, Edward Balkovich of RAND and Jennifer Mnookin of the University of California, Los Angeles, School of Law.

The RAND Safety and Justice Program

The research reported here was conducted in the RAND Safety and Justice Program, which addresses all aspects of public safety and the criminal justice system, including violence, policing, corrections, courts and criminal law, substance abuse, occupational safety, and public integrity. Program research is supported by government agencies, foundations, and the private sector. This program is part of RAND Justice, Infrastructure, and Environment, a division of the RAND Corporation dedicated to improving policy and decisionmaking in a wide range of policy domains, including civil and criminal justice, infrastructure protection and homeland security, transportation and energy policy, and environmental and natural resource policy. Questions or comments about this report should be sent to the project leader, Brian A. Jackson (Brian_Jackson@rand.org). For more information about the Safety and Justice Program, see http://www.rand.org/safety-justice or contact the director at sj@rand.org.

About the Authors

Sean E. Goodison is a senior research associate at the Police Executive Research Forum. His work focuses on research methodology, statistical reasoning, data quality, and violent crime. Prior to joining PERF, Dr. Goodison was a law enforcement analyst within the Executive Office of the Chief of Police at the Washington, D.C., Metropolitan Police Department (MPDC). While at MPDC, he was the primary investigator for a longitudinal homicide case review that collected and analyzed 15 years of homicide data. He has a Ph.D. in Criminology and Criminal Justice from the University of Maryland, College Park.

Robert C. Davis is the Police Foundation's chief social scientist. He has 30 years of experience in criminal justice research and evaluation, and was the Foundation's research director from 2003 to 2006. Davis returned to the Foundation after working as a senior research associate at the RAND Corporation and as research director for the Police Executive Research Forum. Davis has directed more than 45 projects on victimization, domestic violence, policing, crime prevention, immigration, courts, prosecution, and parolee reentry for federal and state governments and private foundations.

Brian A. Jackson is a senior physical scientist at the RAND Corporation and director of the RAND Safety and Justice program. His research focuses on criminal justice, homeland security, and terrorism preparedness. His areas of examination have included safety management in large-scale emergency response operations, the equipment and technology needs of criminal justice agencies and emergency responders, and design of preparedness exercises.

About This Report

On behalf of the U.S. Department of Justice, National Institute of Justice (NIJ), the RAND Corporation, in partnership with the Police Executive Research Forum (PERF), RTI International, and the University of Denver, is carrying out a research effort to assess and prioritize technology and related needs across the criminal justice community. This initiative is a component of the National Law Enforcement and Corrections Technology Center (NLECTC) System, and is intended to support innovation within the criminal justice enterprise.

This document is one product of that effort, completed as a joint effort of the RAND Corporation and PERF. It presents the results of the Digital Evidence Processing workshop, a group convened in fiscal year 2014 as part of the NIJ/NLECTC Priority Criminal Justice Needs Initiative to identify current challenges and innovation needs in digital evidence processing for law enforcement and courts in the United States. This document and the results it presents should be of interest to planners from law enforcement departments, corrections agencies, and courts; research and operational criminal justice agencies at the federal level; private-sector technology providers; and policymakers active in the criminal justice field.

NIJ | National Institute of Justice
STRENGTHEN SCIENCE. ADVANCE JUSTICE.

This publication was made possible by Award Number 2013-MU-CX-K003, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect those of the Department of Justice.

Limited Print and Electronic Distribution Rights

www.rand.org

RAND CORPORATION

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.

RR-890-NIJ