PRESENT: A Framework for Planning and Executing Search Warrants for Digital Evidence

Chad M.S. Steel
Department of Computer Science
Virginia Polytechnic Institute and State University
Falls Church, Virginia, USA
Csteel13@vt.edu

Abstract

The traditional approach to executing search warrants where digital evidence is likely to be encountered is inadequate and outdated. With advances in the miniaturization of storage technology, the prevalence of non-PC devices, and advances in live forensics a new approach is required. In this paper we introduce PRESENT, a framework for planning for and executing search warrants in criminal cases involving digital evidence.

Keywords

Digital forensics; Ecosystem forensics; Live acquisition

1. Introduction

The traditional approach to executing a search warrant where digital evidence is expected to be encountered is outdated and ineffective. Encountering digital evidence is traditionally treated as a special case for the purposes of item collection, and is focused on finding and processing traditional computers (desktops and laptops). The standard approach to executing a warrant (for any offense) is as follows:

1. Perform basic reconnaissance of the physical location where the warrant is to be executed. Examine threats to safety and possible methods of entry/egress.
2. Create an ops plan for the execution. Identify team membership and develop a strategy for the specific situation.
3. Perform entry and clear the location. The entry team announces the warrant, clears the premises, and secures the area.
4. Perform a physical search. After executing entry, split into teams, break up the house into zones, and look for the evidence enumerated in the warrant.
5. Bag, tag, and document the items identified.
6. Examine the physical evidence at the appropriate forensics facility.

While this is a simplification of warrant execution, it is representative of the approach in place at law enforcement entities around the globe. Where digital evidence is expected, a bolt-on approach is taken. In step 2, a digital forensics team may be assigned to the case, frequently without consultation about the execution. In step 4, any personal computers encountered will be shut down (Steel, 2006). These machines will be placed in anti-static bags in step 5, and analyzed by a digital forensics laboratory in step 6.

With the proliferation of non-PC hardware, the increase in the use of encryption, the miniaturization of storage technology, and the presence of a "digital ecosystem" as opposed to discrete devices, the need for a framework that incorporates digital evidence into all aspects of the search is required. We present the PRESENT (Plan, Reconnaissance, Entry, **S**earch, Examine, Notify, and Take) framework as an approach to the handling of digital evidence in a warrant. The framework provides a tool that incorporates digital evidence as a prime concern in all aspects of the search, from planning through execution. PRESENT is meant to provide context to existing methods for searching and seizing digital evidence (Jarrett, Bailie, Hagen, & Judish, 2009), and is presented in the context of the United States legal system, though the approach is applicable to any search with digital evidence, even with differing legal tools available. The approach is meant to be a general approach for all crimes, and builds on previous processes designed for digital investigation by integrating the physical search and interview teams (Carrier & Spafford, 2003).

2. Current Challenges

Changes in technology and the evolution of a digital ecosystem have greatly increased the difficulty in successfully executing a search warrant when electronic evidence is sought. Over the course of the past decade, the approach to individual aspects of digital forensics has changed. Today, most digital forensics teams will do a live analysis of devices encountered, and acquisition of volatile memory is routine (Kornblum, 2007), whereas five years ago a “pull the plug” approach was the norm. Additionally, digital forensics expertise is now more widely available and accessible to search teams in many jurisdictions.

Though the expertise is available and the individual techniques have moved forward, there is a lack of a framework in which to place these advances. Additionally, while procedures have advanced, their ability to address several areas of technology has been outpaced. Several of the challenges detailed below are not well addressed in current approaches, and form a basis for the need for the PRESENT framework.

2.1 Miniaturization

A decade ago, by far the most common digital storage devices encountered were desktop and laptop hard drives and floppy disks. The drives were 3.5” or 2.5” in size, and were found in desktop and laptop computers. The drives could be found with reasonable accuracy by searching for the physical computers, and by removing them from the case. Older drives were likely to be found in close proximity to existing computers, and the devices were generally found in an “off” state, lending themselves to off-site forensics. Floppy disks could be hidden, but had minimal storage that limited what could be stored on them.

Executing a warrant in 2012, the size of storage media has greatly decreased. At the small end, MicroSD cards measure 15x11mm in size (approximately the size of a dime), and are found in everything from digital cameras to smartphones to e-book readers. Currently, 64GB MicroSD cards are available, with 128GB cards on the horizon. Given the large amount of storage and the tendency for individuals to not erase them, small form factor storage is only expected to grow in forensic importance (Szewczyk & Sansurooah, 2011). The new nano-SIM standard for cell phones has an even smaller form factor – 12.3x8.8 mm. Physical searches for devices of this size are nearly impossible, making identification of their likely presence through other means as necessity.[1]

2.2 Encryption

Both full disk and file system encryption have increased in prevalence on devices ranging from Android cell phones to traditional laptops. Hardware-based full disk encryption, as well as easy-to-use software-based encryption such as BitLocker and TrueCrypt, use algorithms that cannot be broken using brute force techniques. Side-channel attacks are much more likely to be successful, necessitating the identification of written passwords and acquiring unencrypted devices which may have forensically recovered text that can be used to build a custom dictionary (Shields, Frieder, & Maloof, 2011).

When the systems are on and unlocked, there is generally a short window for starting the acquisition of data before the system locks and becomes the forensic equivalent of a brick. The ability to quickly lock an encrypted device makes planning critical for when and how a warrant is executed. While cold boot attacks and subsequent memory

[1] There is a benefit to law enforcement with enumeration - the small size of these devices can be used in writing the application for a search warrant to justify searching in containers of just about any size.

analysis are possible in some circumstances (Halderman, et al., 2009), they rely on the preservation of the current power state of a device and expertise not generally found in field digital forensic examiners.

2.3 SSD Devices

Solid state drives are, on the surface, smaller and faster versions of traditional spinning drives. The difference forensically comes with two specific commands – the OS level FORMAT command and ATA8 hardware TRIM command. Both have the potential to rapidly make recovery of data, both in unallocated space and on the entire drive (in the case of FORMAT) impossible.

Traditionally, the FORMAT command is run at the operating system level. Most operating systems when they format the disk only delete the data blocks that contain meta information on the files present (for example, the primary $MFT on NTFS file systems). The data could historically be recovered through carving (or reconstruction of the file system structure information). With SSD drives, doing a FORMAT from the OS may delete the entirety of the drive data (again at the hardware level), leading to a rapid way to wipe content that wasn't available with spinning media.

The TRIM command is used in the background by the SSD to erase unallocated space. Based on the deletion information provided by the OS, the SSD queues up requests for deletion for when there is minimal drive activity. Because of this, a drive that is identified as part of a search may be actively deleting content. Additionally, because this is done at the hardware level, a write-blocker won't help stop the deletion (King & Vidas, 2011)..

2.4 Terabyte Storage Devices

On a standard floppy disk, forensic analysis could be performed using a hex editor and manually reviewing sectors. With the advent of gigabyte-sized hard drives, additional automation from forensic tools was required for analysis. Now, with terabyte-sized hard drives (the current largest single drives available at retail top out at 4TB), even automated tools can't keep up for on-scene analysis.

The time required to image a single drive (or read every sector for analysis) is limited by the maximum transfer rate on the drive and can take several hours. Because of this, selective review of key areas is necessary for on-scene efforts. Additionally, even if the file system is crawled and features extracted (e,g, images), reviewing a gallery on scene, as is the case with tools like Imagescan (used in child pornography investigations), likewise becomes too time consuming. If a 4TB drive stores 1 million images, reading them and reviewing them without more intelligent processing cannot be done in the time on-scene.

2.5 Cloud Storage

Storing data in the cloud, using tools such as Google Drive or Dropbox can make the acquisition of on-scene hardware meaningless. Traditional search warrants are location-limited. If information is sought that is storage off-site at a cloud storage provider, a secondary warrant is needed.

Rapid identification on-scene of cloud storage providers is a must. Because cloud storage can be accessed from anywhere by anyone, a confederate can be actively removing evidence while the scene is being processed. Additionally, and device the subject has access to can be used on-scene or afterward to delete data stored remotely before it is even identified by forensic teams in the lab.

2.6 Digital Ecosystems

The era of the standalone computer is over, and most digital systems encountered are likely to be part of an ecosystem. The Xbox 360 in the living room may be connected to stored media on a desktop in the basement. The iPad is equipped with 4G capability and its data may be stored in a cloud service. The iPod in the dining room been synced with the MacBook in the bedroom. The SD card found in the desk drawer may have originally been in an Android phone, then a digital camera, and finally connected to the Dell Laptop in the office. The photos found on the digital picture frame may also have been uploaded to the navigation system in the Ford Explorer in the driveway. Because devices are connected via networks, both wired and wireless, and because a house can have multiple external connections to the Internet, understanding the connectivity can be as important as examining the stored information. This means that on-scene forensics aren't complete until all of the Internet connections have been identified, and the possible links between devices (and links that are missing devices) are found. Additionally, articulating the ability to connect digital devices in an ecosystem that includes a vehicle, using technologies like Ford Sync, can justify seizure of these non-traditional sources of digital evidence.

3. PRESENT Approach

The PRESENT approach to executing a search warrant digital materials attempts to address the challenges present in the modern IT environment within a home. By incorporating the identification and acquisition of digital evidence into every stage, from planning through execution, the approach is more likely to yield rapid results and the built-in feedback is designed to assist in concurrent interviews on-scene.

The success of the approach relies on the inclusion of a digital forensics team in every phase. The team can consist of a single individual or multiple teams of specialists, depending on digital evidence likely to be encountered. If information is obtained in the early phases of the framework that requires additional expertise, that expertise should be brought in as early as possible.

In addition to the digital forensics team, the PRESENT framework assumes the availability of an adequate digital forensics kit. At a minimum, the kit should include the ability to review and process hard drives, removable media, cell phones, and tablet devices. Additionally, a laptop with a wireless Internet connection and an on-scene printer and scanner are necessary items.

Though the PRESENT frameworks starts with the Planning step of the search warrant, ideally the digital forensics team has been part of the approach from the start.

3.1 Planning

The planning stage of a search warrant is well documented for safety and security (e.g. identifying nearby hospitals, determining a method of entry, etc.) Most planning overlooks the digital forensics needs of the investigation, and is relegated to "add a forensic specialist to the search team". By removing the digital forensic specialist from the planning process, law enforcement teams handicap themselves.

The digital forensics planning process should involve a review of all open source and easily obtainable commercial information available on the subject. Areas to focus on:

- **Technical Acumen.** Does the work/education/usage profile of the subject indicate they are highly technical or a pure Luddite? Articulating a high degree of technical skill or information security background can assist in justifying no-knock, after hours, or sneak-and-peek warrants. If the individual is known to use encryption, the installation of a keystroke logger or hidden camera with the appropriate warrant may be a necessary course of action.
- **Identifiers.** Building a list of online identifiers for an individual will assist in question development, identification of possible targets for electronic warrants/subpoenas, and later forensic analysis. Items to track as identifiers include:
    - *Usernames*. Individuals tend to use the same usernames on multiple systems. Identifying a Skype username may lead to an individual's Amazon.com profile and then to postings on a message board.
    - *Email addresses.* Email addresses provide a target for electronic warrants, and are frequently used as unique search identifiers when issuing a subpoena to online (or even offline) entities. Because many entities, both public and commercial, solicit emails from an individual the possibilities for obtaining addresses from corporate or government sources is almost endless.
    - *Passwords.* Obtaining passwords or personal questions/answers used by a subject from other sources can assist in password guessing attacks against encrypted systems encountered later. It is rare for an individual to *not* reuse a password or permutation thereof on multiple systems (Ives, Walsh, & Schneider, 2004).
    - *Phone numbers.* Phone numbers may provide subpoena targets, which may lead to other identification information. Mobile phone subpoenas, in addition to providing basic subscriber information, will almost certainly provide an email identifier if asked for. Additionally, knowing the level of data plan on a mobile phone and feature usage (such as tethering) are critical in identifying the subject's methods of Internet access and for identifying device targets for the physical search. Call detail records (CDRs) can provide location information on where a subject is as a particular time.

  - *Online activity profiles.* The trap-and-trace is a frequently overlooked investigative tool for digital forensics. Aside from the basic connection information provided, using a trap-and-trace on the ISP can show when an individual is online, which in turn can be used in planning when to execute the warrant.
  - *IP Addresses.* Finding the IP addresses that an individual has used, especially if they are static, can be useful in both geolocating where an individual connects from (e.g. does the IP return to a Starbucks in De Pere or a Marriott in Spartanburg) and for determining if an individual is openly sharing information (by connecting to the IP they are currently using).
- **Technology Purchase History**. Finding where an individual shops allows for their technical purchase history to be obtained via subpoena. If an individual leaves reviews of products on Newegg.com, its likely they purchase their computer hardware from there. Additionally, if they are asking questions on an Apple message board, they likely have an iTunes account. By issuing subpoenas from these merchants, the search team can identify products to look for during the search.
- **Social Network Information**. Publicly available information on the social networks the subject belongs to is useful in obtaining additional details on the items noted above. An iterative Google search on permutations of the person's name and other identifiers as they are found can lead to the development of a full profile on an individual in a completely non-invasive manner. Subpoenas for records from Twitter, Bebo, or Facebook can provide early context on an individual's digital activities.

Because the PRESENT approach relies on integration with the traditional investigative team, any information obtained by the digital team should be shared. Information on group memberships, associates, friends, and interests can assist an interview team and may help draft approaches in other areas of the warrant execution. It is also the responsibility of the digital forensics team to create a list of unanswered technical questions for the interview team to address with the subject. This list will be revised and updated in later stages.

3.1.1 Output

The products of the Planning stage for digital evidence purposes should include the following:

- A list of known products containing digital evidence to be seized.
- Identification of the appropriate expertise to bring for on-scene forensics given the list above and the technical profile of the subject.
- A determination of the best times, based on usage, to execute the warrant.
- All of the potential usernames, passwords, and biographical information available on an individual to assist with later forensic review.
- A list of interview questions related to the usage of the items identified above.

3.2 Reconnaissance

Standard reconnaissance for any warrant is iterative with the planning stage. Reconnaissance activities are differentiated from planning activities in that doing recon has the potential for discovery[2]. For the purposes of digital evidence in a search warrant, recon can be divided into two phases – physical and logical.

3.2.1 Physical Reconnaissance

As with all search warrants, a thorough visual inspection and imaging of the subject's residence is needed. Standard recon photographs cover possible approaches for entry (and exits), threats to the team, and details of the location for the warrant application.

For digital evidence purposes, additional relevant information can also be gathered at the time of the physical reconnaissance. The presence (or absence) of cable boxes can give an indication of Internet connectivity at the home, and information on a potential ISP. The demarcation point for any physical access (the place the coaxial or fiber cable, or satellite dish connection, enters the house) should be noted.

Wireless access can and should be enumerated as part of the physical recon stage as well. Use of a laptop and wireless card with Netstumbler (or similar tool) will provide a view of local wireless access points. Any open (or secured) access points present at the home, including their SSIDs and manufacturer, should be identified.

[2] Executing certain provisions of 18 USC 2703 in the United States, including the issuance of preservation notices, can potentially trigger unwanted notifications to the subject. The US Department of Justice Computer Crime and Intellectual Property Section (CCIPS) maintains a list of law enforcement guides for many entities that retain computer data and can provide guidance to law enforcement on this issue.

Additionally, any open wireless access points in range of the home should be identified. The use of a directional antenna can help to associate specific access points with a specific residence. Enumeration should end at the identification of the devices and care should be taken not to capture any data packets to avoid potential wiretap concerns.

3.2.2 Logical Reconnaissance

Logical recon is an attempt to ascertain relevant warrant execution information using semi-invasive online techniques. These involve connecting to devices owned by the subject or engaging with the subject in an undercover fashion in ways that may reveal the investigation. As with physical recon, the value of the information obtained should be weighed against the risk of being caught.

A low-risk preliminary step in logical recon is the attempt to engage the subject over social networks. If the subject has a Facebook, Google+, LinkedIn, Bebo, or other social networking profile, viewing that information with an undercover account is considered non-invasive. As users become more privacy conscious, it is becoming increasingly necessary to be a member of a person's network to view much of the information of investigative value. Creating a profile that would likely be friended by the subject, and even approaching people in the subject's network in an undercover fashion online, may be warranted for search purposes. Once accepted into the network, the interest profiles, employment history, and education may provide clues as to the tech savvy and digital activities of the subject. Additionally, photos posted can be analyzed for search planning purposes, and the EXIF information on them exploited to identify devices and locations to search.

If the case involves file sharing, connecting to any shared files and obtaining evidentiary copies of them can be done at this point. US courts have held that connecting to an individual's machine that is publicly sharing files over peer-to-peer is acceptable (United States v. Stults, 2009), and obtaining digital evidence in this fashion can be used to support planning or probable cause.

Case-specific logical interactions may be necessary at this point as well. Engaging in an undercover chat with a subject, sending the subject targeted emails to elicit behavior, or installing monitoring software on the subject's devices (with the appropriate legal procedures) may be done depending on the specifics of the case.

3.2.3 Output

The products of the Reconnaissance stage for digital evidence purposes should include the following:

- A list of likely ISPs and an annotation of where they physically enter the location
- An enumerated list of potential wireless access points, but inside the residence and nearby
- An updated list of items to be seized inside the residence, based on online profiles

3.3 Entry

Entry is concerned primarily with obtaining access to the residence and securing the scene. In a typical warrant, the entry team stacks up on the door, knocks and announces their presence, then enters the location. The warrant is served during daytime hours, and there is a small delay between knocking and obtaining access to the interior.

There are two primary considerations with digital evidence in the entry plan. First, the need for a non-traditional entry should be evaluated if the subject is likely to have encryption or the subject is likely to quickly destroy evidence. Second, the entry team should be trained to recognize systems that may go into sleep/hibernation mode or lock if not immediately secured.

3.3.1 Approach

Ideally, all digital media will be encountered up-and-running and unlocked. With creativity, the entry team can enhance their chances of this occurring. First, by articulating the likelihood of encryption and a technically sophisticated subject, a no-knock warrant can be sought. Based on the information obtained in the planning and recon stages, a no-knock can be executed at a time when the subject is likely to be using target systems of interest (and it never hurts to catch them "in the act" if the crime itself is digital in nature).

If a no-knock warrant isn't available, the entry team should consider a ruse to bring the subject out of their home. Making a pretext phone call (which has the benefit of the subject potentially possessing an unlocked and active cell phone) to bring the subject outside the location is preferable, as the subject may lock their systems when answering a knock at the door. If neither of these are possible, the entry team should be trained to identify any active digital evidence immediately after securing the location.

3.3.2 Entry

Many current digital devices have a limited amount of time before they become inaccessible without the use of a password. Cell phones may lock in a matter of 30 seconds, whereas a laptop may go into sleep mode after 5 minutes. Because of this, rapidly securing and maintaining the state of a device takes precedence over everything except safety and security. Traditionally, digital devices were treated like any other piece of evidence. Once the search teams found the evidence during the normal course of the execution, the devices were shut down, bagged and tagged. The delay for active devices, given the current state of encryption and the volatility of information, justifies a more immediate approach.

First, the entry team should ensure the subject and others present do not have access to any digital devices that may allow them to initiate the destruction of information. This includes cell phones, computers, tablets, and other digital devices. Second, any active devices encountered by the entry team should be immediately identified and the necessary steps taken to ensure they remain active. For a cell phone, this may mean touching areas of the touch screen that are unlikely to impact the underlying data. For a laptop or desktop, it means moving the mouse or using a tool such as the Mouse Jiggler™ to maintain the active state. While there is the small possibility of altering evidence with this approach (including physical evidence – e.g. fingerprints and swipe patterns on a touch screen), it is outweighed by the exigent need to avoid complete data "destruction" through its unavailability.

After the active electronic devices are secured, a means of ensuring constant power should be the next priority. The means may range from asking the subject for the location of a charger to prioritizing the finding of power adapters to using charging tools from the digital forensics toolkit.

3.3.3 Output

The products of the Entry stage for digital evidence purposes should include the following:

- The subject and other present are separated from digital devices
- Any readily identifiable, active digital equipment is stabilized and powered for further analysis

3.4 Search

The PRESENT framework Search step is iterative with the Examination and Notification steps, and encompasses both physical and logical searching procedures. In a typical search, the digital evidence is identified as part of the physical search procedures. The PRESENT approach allows the search team without digital specialization to proceed with the physical search, while permitting the digital evidence specialists to focus on identifying items that they can exploit on-scene and provide the physical search teams with the immediate results of exploitation. The steps presented do not preclude following standard evidence handling procedures (photographing, documenting, and handling appropriately) and chain of custody requirements.

3.4.1 Network Identification

Instead of beginning the search for physical storage devices, a more effective approach is to identify connectivity equipment and then find those devices that they interact with. If a physical Internet connection is identified in the Recon step, that should be the first stop for the digital forensics specialist. The connection is likely to terminate at a router (with a modem or other translation device in between) which can be used as a starting point for identifying network devices. If the router has physical connections, these can be traced to connected devices. If it is purely a wireless device, exploiting it to obtain connection logs can be performed to identify machines to search for. The exploitation mechanism will be device-specific, and is covered in the Examine step.

After identifying the wired Internet connection, wireless connections should be identified. This may consist of cell phones, 3G/4G network access cards on computers, or tablets with built-in wireless connectivity. These devices are most likely to be found by a physical search, and should be the next priority for the Examine phase.

3.4.2 Device Identification

Device identification should focus on items found during the physical search which may have digital storage capabilities. Once a device is found, it should be triaged to ensure the expected digital storage is present. Any digital storage that is missing (e.g. a computer without a hard drive, a camera without an SD card) should be listed on the potential seizure list and provided to the search teams as items to seek out. Similarly, storage devices without any associated processing unit (e.g. a SIM card without a phone) should also be noted.

Because of the small size of digital devices, search teams should open all available containers and pursue all reasonable hiding spots. While searching for the devices, any papers which may contain passwords should be documented, and any manuals or paperwork for devices not present should be noted. Any chargers or cables found should be seized, and if the associated item has not already been found it should be added to the list.

3.4.3 Output

The products of the Search stage for digital evidence purposes should include the following:

- A checked-off list of digital evidence items seized and digital evidence items yet to be found

3.5 Examine

Because of advances in digital forensics, many search teams now have the capability of doing on-scene live analysis of devices found. This analysis should focus on items that will be of immediate value – both for preservation of evidence and for feedback to the search and interview teams. Preservation should focus on the most volatile information (generally RAM and activity logs) first and be done consistent with sound forensic practices.

With standard hard drives, connecting to a hardware write blocker was the accepted practice for many years in digital forensics. Because of the inability of a write blocker to avoid data alteration on SSDs, and because of the diversity of digital items encountered, write blocking may not be possible. As such, in-situ analysis is becoming more necessary, and is a valid and accepted practice. In-situ analysis may include running tools off a known-good CD, manually navigating a smartphone menu, or mounting an SD card read-only to a Linux laptop. As with most forensic techniques, every analysis should be well documented and ideally observed by a second individual.

Due to the large amount of storage that is frequently encountered, exhaustive on-scene forensics is not likely to be possible. For the purposes of PRESENT, the priorities in examination should be set to preserve the most volatile data first, and to analyze for the following:

- *Network connections.* Identification of any networks that a device is (or was) attached to will show where it fits into the digital ecosystem. Additionally, the networks themselves can then be connected to and enumerated to identify additional devices of interest. Network connections should also include cloud storage services, social networks and email connections. Identifying these will be helpful in the Notify step below.
- *Devices.* Any devices that have been recently attached to a digital evidence item should be enumerated. Devices may be found by looking at everything from USB mass storage devices shown in the Windows registry to an iPhone profile found on a MacBook. Because any devices not seized while on-scene are subject to later alteration or destruction, it is critical to identify possible targets before ending the search.
- *Recent Activities.* Showing what an individual was doing just prior to the search can provide clues to other pieces of volatile information. Most-recently-used (MRU) lists and activity logs provide the most valuable insight into recent actions.
- *Crime-specific Activities*. Identifying specific evidence of the crime in question is generally the first thing done, but once seized and appropriately secured, the evidence will remain for future analysis. Any searches for evidence of elements of the crime should be focused on finding things that will be helpful to the interview team in the Notify step.
- *Barriers to Access*. Encrypted files, inaccessible areas, and locked devices encountered can be fed to the interview team as questions to be addressed. Specific access controls may require additional Search actions – finding a login that looks for a SecureID token number or encountering an Android phone with a face locking features may require additional searching or taking a digital photograph of the subject, respectively.

3.5.1 Output

The products of the Examine stage for digital evidence purposes should include the following:

- An updated list of devices not yet found
- A list of questions to ask the subject based on identified activities or obstacles encountered (e.g. an encrypted drive)

3.6 Notify

Notification is a two-way process between the interview team and the forensics team. Notification can be done at a set time (the interview team takes regular breaks to consult with the forensics team) or on-demand (the forensics team interrupts the interview with critical information). With either approach, the rules for that particular search should be agreed beforehand by the entire team.

3.6.1 Interview Team

The confrontational interview of the subject should occur simultaneously and in close proximity to the search, but be physically separated from the activities of the search team. Ideally, the interview can occur inside an already-cleared room within the location of the search. Alternatively, a simultaneous interview offsite can be coordinated though active communication between the search and interview teams.

In addition to the questions relevant to the crime being investigated, the interview team can obtain several pieces of information that are relevant to the search team. Questions that can be asked include:

- How do you connect to the Internet?
    - What do you do when you are online?
- What is your primary email address?
    - What other email addresses have you used?
- What social networks do you belong to?
    - What account names do you use?
- What cell phones/computers/tablets/digital cameras do you own?
    - Do you password protect them?
    - With what password?
    - Where are they?
- How do you backup your data?
    - Where are those backups located?
- Do you use encryption?
    - What password did you use to encrypt your devices?

The answers to the questions should be provided to the digital forensics team for confirmation and corroboration. Additionally, the subject should be asked about any digital forensic items identified during the search, any passwords or usernames encountered, and any items on the list created that are not yet found.

3.6.2 Digital Forensics Team

The digital forensics team, in coordination of the search team, should prepare a list of questions that arise during the Examine stage above and provide them to the interview team at the appropriate time. Any usernames/passwords, unusual devices, or barriers to entry encountered should be fed to the interview team as required information to obtain from the subject.

Any information that is obtained during the above phases or by the interview team regarding online accounts should be used to generate preservation notices to send to the appropriate providers via fax or email. By generating and sending the notices immediately, any confederates that have access to the subject's online information (or the subject themselves if the interview is non-custodial and is terminated) will not be able to destroy future digital evidence.

In addition to preservation notices, the digital forensics team should generate consent forms for access to all of the online services enumerated above. The consent forms should include a space for the username and password used, and should be provided to the interview team for signature by the subject at that appropriate point. The consent should give the digital forensics team the ability to access and obtain any and all information stored in the account. Ideally, the information provided can be verified before ending the search. If the case involves other subjects, consideration should be given to obtain consent to *take over* the account in lieu of just accessing it.

3.6.1 Output

The products of the Notify stage for digital evidence purposes should include the following:

- Locations/information on all digital forensics items identified but not found
- Preservation notices sent to all identified online providers
- Signed consent forms for all online services
- Usernames/passwords for all protected devices.

3.7 Take

Generally speaking, any items explicitly called out in the search warrant can be taken. Additionally, any contraband or other items that are found in plain view during the search and may be evidence can be seized as appropriate under exigency and a second warrant sought either telephonically or in person for them. Although the warrant may give the team the right to seize the items, the team should triage digital evidence items on-scene into several categories before deciding what to remove:

- *Items to Seize*. Items that either have been found to contain evidence or are likely to contain evidence and cannot be examined on scene.

- *Items to Clear*. Time permitting, items which can be easily reviewed and cleared on-scene should not be seized. Stacks of CD/DVDs, digital cameras, memory sticks, and other items that can be quickly reviewed on-scene should be examined and cleared.
- *Items to Ignore*. Items predating the criminal activity or that are not likely to be used to store relevant data can be ignored. Stacks of old floppy disks (in a recent crime) and commercially stamped (as opposed to burned) DVDs are examples of items that can generally be ignored.
- *Items to Image*. This includes items that will remain (and not be seized) as well as items that require imaging of their volatile areas before being packaged for seizure. In a corporate environment where there is an individual subject, there may be a reason to image storage in place and leave the devices. Similarly, a laptop without a charger may need to have its memory rapidly imaged, even though the device will be seized for full analysis at a later point.

Once the items identified have been bagged-and-tagged, they can be entered into evidence and processed in the lab environment. Packaging of the materials is item specific and may include anti-static bags, Van Eck shielded storage, or portable power supplies depending on the item.

3.6.1 Output

The products of the Take stage for digital evidence purposes should include the following:

- All digital items requiring further processing or found to contain evidence of criminality

4. Conclusions

By thinking about digital evidence as a core component of searches, law enforcement maximizes their ability to successfully solve both computer and non-computer crimes. With the further integration of digital evidence teams, evidence that may have been previously left behind or overlooked will, in the future, be seized and assist in prosecuting (or exonerating) subjects of criminal inquiries.

The PRESENT framework provides the first digital-evidence specific method of organizing and executing a search warrant. It is meant to supplement and not supplant existing search warrant procedures, and is flexible enough to change as the digital landscape changes.

5. References

Carrier, B., & Spafford, E. (2003). Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence , 2* (2).

Halderman, J. A., Schoen, S. D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J. A., et al. (2009). Lest we remember: cold-boot attacks on encryption keys. *Communications of the ACM , 52* (5), 91-98.

Ives, B., Walsh, K., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM , 24* (4), 75-78.

Jarrett, H. M., Bailie, M. W., Hagen, E., & Judish, N. (2009). *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* Department of Justice Office of Legal Education.

King, C., & Vidas, T. (2011). Empirical analysis of solid state disk data retention when used with contemporary operating systems. *Digital Investigation , 8*, S111-S117.

Kornblum, J. (2007). Using every part of the buffalo in Windows memory analysis. *Digital Investigation , 4* (1), 24-29.

Shields, C., Frieder, O., & Maloof, M. (2011). A system for the proactive, continuous, and efficient collection of digital forensic evidence. *Digital Investigation , 8,* S3-S13.

Steel, C. (2006). *Windows forensics: The field guide for conducting corporate computer investigations.* Wiley.

Szewczyk, P., & Sansurooah, K. (2011). A 2011 investigation into remnant data on second hand memory cards sold in Australia. *Originally published in the Proceedings of the 9th Australian Digital Forensics Conferenc.* Perth, Australia.

United States v. Stults, 08-3183 (8th Circuit 2009).