Chapter 10
Executing a Search Warrant for Digital Evidence

Chapter Outline

I. Once a search warrant is signed and the pre-planning phase is over, the planning for the actual seizure can begin.
II. Investigators not familiar with computers seek out the assistance of someone who is familiar with the latest in technology.
   A. Local computer experts.
   B. Colleges and universities' computer sciences departments.
III. Properly powering down a computer and packaging the various components of the computer system is as important to the successful prosecution of a case as are the other stages of the criminal investigation.

I. The Steps of Executing a Search Warrant for Digital Evidence
   A. Step One: Removing the Suspects from the Computer
      1. Executing a search warrant for digital evidence is much like executing a search warrant for any other contraband evidence.
      2. There is a greater potential for the suspect to damage or completely destroy any evidence when it is digital in nature.
         a. Computers that are powered on can allow the suspect to use a variety of software programs that will either encrypt evidence or destroy evidence.
         b. Like any emergency preparedness plan, the best plans for handling digital evidence are always prepared with the idea that such programs will be encountered during the collection of digital evidence.
      3. Some have questioned whether "no-knock search warrants" should be obtained when executing a warrant for digital evidence, but it is hard to meet the criteria of officer safety for such a warrant.
      4. There are two methods one could remove a suspect from a computer:
         a. By asking the individual to shake your hand and preventing them from returning to the computer.
         b. Through the use of physical force.
      5. It is very important that the suspect not be allowed to return to the computer for any reason.
   B. Step Two: Securing the Scene
      1. From the instant the suspect is removed from the computer, the focus should be securing the scene and beginning the process of documenting the crime scene.
      2. Photographs may become an important part of the case later on should the suspect decide to pursue a jury trial.
         a. It is recommended that personnel use a digital camera to take these pictures.
            i. Saves money because there no need to buy film.
            ii. Allows investigators to ensure good usable images while on

the scene.

3. One technique that has become much more commonly encountered as video cameras have dropped in price is the use of a digital camera to record the entire search.
    a. Useful should the suspect attempt to claim that the digital evidence was planted by law enforcement officers.
    b. Allows for a more thorough documentation process
        i. Can provide a 360-degree view of the suspect's computer(s).
        ii. Can provide a view any peripherals attached to the computer(s).
4. It is important to take pictures of the suspect's computer(s) at the time the search warrant is executed.
    a. Allows investigators to go back later and document exactly what programs were operational at the time of its seizure.
    b. Used to counter a suspect's argument that they were not engaged in a particular activity.
5. In most cases it is also recommended that the photographer obtain a picture of the time stamp located at the bottom right-hand side of most computer screens.
    a. Can be used in cases in which multiple people have access to the machine to determine who was using the computer at the time of the illegal activity.
    b. It is also recommended that investigators make note as to whether the time is correct, so that if the time is incorrect, forensic analysis can reconcile any activity logs.
6. Investigators must be sure to provide a brief training session with any individuals who will be assisting with the search who may have limited experience executing search warrants so that evidence is collected properly.

C. Step Three: Disconnect any Outside Control Possibilities
1. When locating network connections within the residence, it should be noted that wireless networks are more than likely to be encountered.
    a. These wireless networks can be problematic in that there is a need to immediately shut off any network connections in order to remove the possibility of someone outside of the residence damaging potential evidence.
    b. An investigator should familiarize himself/herself with the latest wireless routers prior to executing a search warrant.
    c. Network detector programs (such as those found in cellular telephones) can be used to detect the presence of wireless networks.
2. There is a chance that an investigator will also encounter a computer connected to an Internet via a telephone line.
3. Regardless of whether the Internet connection is via a narrowband or broadband connection, an investigator should disconnect the Internet

connection as soon as possible.

4. Investigators should be aware that there is a possibility that the network is not connected via the connection closest to the computer.
5. Following the terrorist attacks of September 11, 2001, there was a movement among some companies to allow evidence to be stored at a location different that where the computer normally operates such as:
    a. Data storage services
    b. Intra-company networks
    c. Data hosting services
    d. This means that the digital evidence an investigator is searching for may be stored on a computer across the street, across the city, or across the country.
    e. Digital evidence that the investigator is searching for can be stored on a computer across the street, the city, or the country.
    f. In ideal scenarios investigators would have knowledge of such off-site storage of data prior to the development of the search warrant.
        i. If such information is not available, then there will still likely be some evidence on the seized computer showing where the data is stored.
6. Before disconnecting a computer from the Internet or network, the investigation should look for the presence of active downloads.
    a. An investigator may make the decision to photograph or video record the screen of the computer and include notations concerning any programs or files that are currently downloading or recently downloaded.
    b. Investigators must be aware of the fact that any utilities running can be minimized at the bottom of the screen, and if the decision is made to maximum the screen, the investigator must ensure that his or her actions are recorded in the search log; if possible, the entire process should be videotaped.

D. Step Four: Powering Down the Computer

1. An investigator executing a search warrant for computer-related evidence will have to consider which operating system, and version of the software, the user is running on the computer.
    a. Version and brand will determine the proper method of powering down the computer.
        i. Using the operating system's shutdown features
        ii. Unplugging the power cable from the back of the computer
    b. Pulling the plug from the back of the computer is considered the most effective means of properly powering down the computer.
        i. This prevents any malicious software or code launching when the computer is shut down.
        ii. There are software programs available that begin formatting a computer's hard drive if proper shut-down protocols are not adhered to, but the use of such programs is rare.

2. Before a decision is made to power down the computer, it is important to examine the computer to determine whether there are any programs running on the computer, because potential evidence could be damaged.
    a. This requires familiarity with the various operating systems, which helps an investigator determine whether there are any files open and stored in the computer's Random Access Memory (RAM).
        i. Data that is stored in RAM memory will be lost when the computer is powered down, and such data is not normally recoverable.
        ii. If programs are found, the decision to save the file or shut down the computer and lose data can be made.
3. Microsoft Windows operating system is likely to be the most commonly encountered operating system.
    a. Software programs and files that are open and running can be located by looking at the bottom of the computer screen.
    b. An investigator who chooses to save a copy of the file should ensure that the file's name is one that they can easily remember and one that can easily be explained to a judge and a jury should the need arise.
        i. A note in the search log should be made of the file name selected, as well as the time the file was discovered and the time the file was saved to the external drive to prevent the corruption of evidence stored somewhere else on the suspect's hard disk.
4. If the suspect is running a version of Linux, then the method of determining whether there are files running in RAM may be different.
    a. Recently there have been Windows emulators (sometimes referred to as WINE) that allows users to run applications in much the same manner as those in Microsoft Windows.
    b. If, however, the suspect is running the Linux operating system in Command-prompt mode, an investigator must type "ps" to get a list of programs running in RAM from the command line prompt.
        i. Files of importance need to be saved before shutting down the computer.
        ii. Saving files via command line interface can be complex, and as such, it is recommended that the individual on scene merely shut the computer down if assistance cannot be obtained from someone trained in the use of Linux.
5. Once all files running in RAM have been handled, the next step is to power down the computer.
    a. Determining the operating system and version must be considered before deciding how to power down the computer.
        i. Windows Operating System
            1. Newer versions have become less susceptible to damage or loss of data from losses of power—meaning that powering down the computer has

become much easier and requires less technical skill.

2. The majority of Windows operating systems are best powered down by merely pulling the plug from the back of the central processing unit (CPU).
    a. To prevent devices that are programmed to deliver high-voltage surges of power from damaging the CPU's internal components.
    b. Only the Windows 2000 Server requires the computer to be shut down using proper shut-down features in the operating system.
3. In most cases, the operating system the computer is running can be easily identified.
    a. Identifying operating system:
        i. Access an icon labeled "Start" at the bottom left side of the computer monitor
        ii. Right clicking the option labeled "My Computer" will bring up the option "Properties"
        iii. The "Properties" option displays information on the computer and the operating system.
    b. Some of the earliest versions of the Windows operating systems (generally Windows 95 and early versions of XP) will maintain banners that identify the operating system version in a vertical format.
        i. Visible when users select the "Start" tab from the bottom left side of the screen.
    c. If after trying to determine the operating system and version, the investigator is unable to determine which version of the software is running, then the plug should be removed from the back of the computer.
4. Operating systems that cannot be powered down by pulling the plug from the CPU can be shut down easily through the use of the internal features of the software.
    a. Selecting the "Start" icon.
    b. Select the option "Shut Down" or "Turn Off Computer."

ii. Macintosh Operating System

1. The Macintosh operating system is currently used in the Macintosh line of computers that are manufactured by Apple Computers.
2. International Business Machines (IBM) was an early manufacturer of computers, and their design and software protocols were the ones more commonly encountered in the early days of computing.
3. Today, there is more interoperability because software manufacturers produce software that is available for both IBM-style computers and Macintosh-style computers.
4. Newer versions of the operating system are better capable of recovering from immediate power loss.
5. Older versions of the Macintosh operating system, however, require the computer to be properly powered down through the use of the internal commands built into the operating system.
6. The video-editing capabilities of these computers may increase the chances that these computers may be encountered when investigating cases involving digital child pornography.
7. Files stored in RAM may not be as easily located on the Macintosh operating system.
    a. Earlier versions of the Macintosh operating system required the user to select the "Finder" option at the top right hand side of the computer screen to see which files or programs are running.
    b. Once the files are located, then the investigator can decide whether to save the files or shut the computer down without saving the file to an external storage device.
        i. The computer can be powered down by selecting the "Special" option from the top menu bar of the screen and selecting the option "Shut Down."

iii. Unix/Linux Operating System

1. The UNIX operating system has been in use for decades and is a very popular operating system to be used for operating network servers that host Internet websites and web-based software.
2. Investigators who encounter users running the Linux or Unix operating systems must be very careful when shutting down the computer.

3. These operating systems do not allow for sudden losses of power.
4. Computers that are running the Linux command line operating system—identified by a non-graphical screen with text only on the screen—can shut down the computer by typing the command "shutdown h now" at the command prompt.
5. If an investigator encounters a computer running a windows-like operating system such as the Linux Windows X program, then shutting down the Windows-based operating system does not turn off the computer but instead returns the user to the command prompt.
6. Another important reason for properly powering down a computer running the Linux operating system is that some versions of the software save the last 100 commands that a user types into the command prompt, information that can be useful in investigating computer intrusion and hacking attacks.
7. This operating system is more prone to software booby traps than that of Windows and Macintosh operating systems, and it is for this reason that special care should be taken when dealing with computers that are found to be running the Linux operating system.

6. Laptop Computers
   a. With the increase in popularity of laptop computers, there is an greater likely of encountering them in the investigation of cybercrimes.
   b. Laptops are different from desktops in that laptops operate on a dual source of power.
      i. Operate on AC power (using a power cable plugged into an outlet) and a battery backup when AC power is unplugged.
      ii. Powering down a laptop entails unplugging the power plug from the rear of the laptop and removing the batteries
   c. In terms of handling the various operating systems for laptop computers, the previous discussions still hold true.
   d. If an investigator desires to leave the computer running after securing the scene, then it is important to ensure that there are no wireless networks operating in the area.

E. Step Five: Disassembling the Computer
   1. If there is only one computer, then there is obviously less potential for problems at this level, but multiple computers require personnel to disassemble computers in such a manner that the investigator can later reassemble any or all of the computers in a lab or in courtroom should

the need arise.

2. It is recommended that each cord or device be labeled as it is being unplugged from the back of the suspect's computer.
    a. Should the investigator encounter ports that are not in use, the port should be taped and labeled as not in use.
3. Some investigators found the use of masking tape fine for labeling seized computers, while others like to use colored labels.
    a. Using colored labels can be useful in the seizure of multiple computers because each computer can be color-coded.
4. Once the computer is disassembled, then investigators need to examine the area for additional hardware that could be potential evidence.
    a. Types of hardware that could contain useful evidence
        i. Digital video camera
        ii. Videotape, CD-ROM, DVD-ROM
        iii. Scanner
    b. The decision as to how much of the peripheral equipment should be seized is a question to be answered by (1) the investigator's determination based upon facts of the case, and (2) the search warrant authorizing the seizure.
        i. Seizing all peripheral equipment can be useful if the computer forensic examiner needs the original parts to reconnect the computer or if the investigator is asked to reassemble the computer at a later date.

F. Step Six: Securing Additional Evidence from the Scene

1. One of the primary concerns is whether additional evidence is included in the application for the search warrant.
    a. If not, the investigator must prove that the seizure is necessary based on one of the warrantless seizure exceptions.
    b. Items included in the search warrant should include floppy disks, flash drives, external hard drives, manuals, and other electronic storage devices, as well as paperwork devoted to the computer systems in use.
2. Once these materials are seized, they should be taken to an individual who has been pre-selected to catalog the evidence seized at the scene to make sure that the disks are write-protected (no data can be added or deleted).
    a. Decrease chance of a mistake being made during the imaging process.
    b. The device should be labeled with information such as room/location in which it is found, who located it, and any necessary additional information.
3. Along with digital storage devices, CD-ROMs and DVD-ROMs, personal data assistants (PDAs) and other handheld organizers, and smart cellular phones should also be considered during a search.
    a. Each of these devices can be connected to an owner's computer, and files can be moved between the two devices.
    b. These devices can be recovered anywhere around the premises.

4. Once the search for storage media is completed, then investigators should begin examining manuals that surround the computer.
    a. Manuals can help with understanding the various programs on the computer to retrieve digital evidence.
    b. Manuals also can be used to obtain passwords necessary to access protected programs.
5. Finally, during the search for manuals it is important that investigators consider the possibility of locating a listing of passwords.
    a. Investigators should search under, over, in, and around the area where the computer was stored.

G. Step Seven: Preparing the Evidence for Transportation
1. Once all of the evidence has been collected, the individual assigned with the task of logging the evidence should verify that the asset seizure log has been completely itemized so everyone is aware of exactly what items have been seized.
    a. Copies should be made for the agency and the suspect.
    b. Completed forms should be signed by the suspect, but if the suspect refuses, it should be noted and signed by the officer in charge.
    c. Evidence seized should be listed on the form by lines, with each item seized occupying its own line.
2. Upon completion of the asset seizure form, the investigator should begin preparing to ship the computer back to the evidence vault.
    a. Plastic bags or boxes are generally used to store evidence.
        i. Hard drives an storage media should be maintained in a static-free bag in order to prevent damage to the contents.
        ii. Styrofoam should be avoided as it provides the possibility of static electricity that could damage the computer or the storage media within the device.
    b. Any empty disk drives should have blank evidence disks inserted to prevent damage during shipping.
    c. The computer should not be placed in the trunk of the police car because of heat and the electric discharge of equipment stored in the trunk of many police cars.

II. Wrapping Up the Search and Preserving the Evidence
A. Once all of the evidence is seized, properly logged, and packaged, it becomes important for the investigator to ensure that the evidence is secured in such a manner that it can be presented in court at a later date.
B. Understanding the Chain of Custody
1. Digital evidence that is left unsupervised can be completely erased and modified in a short amount of time and require additional care during the preservation phase while awaiting the trial.
2. An investigator should be able to provide information on any individual and/or agency that has handled the evidence for the investigator, stretching from the time the evidence is seized until it is present as evidence at trial.
3. Because every individual who has touched the evidence must testify to the

evidence being the original evidence, there are several opportunities for the defense to have the evidence removed if there is a problem with determining who has touched the digital evidence.

a. Defense may question why the individual touched the evidence.
b. It is suggested that an evidence transaction log be maintained when investigations involve the presence of digital evidence.

III. Conclusion

Key Terms

Broadband Internet connection: A connection to the Internet via DSL, cable, or fiber optics.

Chain of custody: The ability of an investigator to provide information on any individual and/or agency that has handled the evidence.

Evidence transaction log: A log that contains information related to who removed digital evidence from the evidence storage facility, where the evidence was handled, and why the evidence was removed from the secure area.

Narrowband Internet connection: A connection to the Internet via a telephone line.

Network detector program: A program with the ability to detect the presence of nearby wireless networks.

Temporary folders: Folders used to store data that has not been properly saved by the user.

Write-protected: No data can be added to or deleted from a disk