

Field Guide Part Six

Timothy E. Wright 2000-01-08

The Field Guide for Investigating Computer Crime, Part Six: Search and Seizure - Evidence Retrieval and Processing

by *Timothy E. Wright*

last updated Jan. 8, 2000

In Our Previous Episode...

In our last article, "[Search and Seizure: Approach, Documentation, and Location](#)" we saw how a team of investigators interacts with the computer crime scene during the stages of securing and documenting the crime scene, and searching for evidence. Up to this point, the process of search and seizure hasn't been overly cumbersome - below, the discussion of evidence retrieval and evidence processing will change this! Not to despair, though. As we mentioned in the second article, "[Overview of a Methodology for the Application of Computer Forensics](#)" , it is possible to streamline the effort of investigating computer crimes. For example, an organization might assign degrees of priority to cases, such that the most urgent cases require a full treatment by investigators, while the least urgent do not. The key here, is that an established policy governs the assignment of priorities to cases, and guides the investigative process accordingly.

Let us now consider the last two stages of search and seizure, starting with evidence retrieval.

Retrieving Computer Crime Scene Evidence

| | | | | | |
|-----------------------|--|------------------------------------|----------------------------|--------------------------|-------------------------|
| (A) | (B) | (C) | (D) | (E) | (F) |
| Formulate plan | Approach and Secure Crime Scene | Document Crime Scene Layout | Search for Evidence | Retrieve Evidence | Process Evidence |

Figure 1: Retrieving Evidence - Stage E of a Search and Seizure

After the initial search of the crime scene, any computers, devices, and media that have been

located are ready to be documented and prepared for transport back to an evidence preservation lab. The process consists of the following sequence of steps:

1. start the search and seizure evidence log;
2. document computers, devices and media;
3. determine whether or not to power down computers;
4. power down computers;
5. mark and tag all hardware, cables and media;
6. prepare computers, devices and media for transport - start the shipping manifest;
7. transport computers, devices and media;
8. unload computers, devices and media;

Step 1: Start the Search and Seizure Evidence Log

In addition to photographs and sketches of the crime scene, a detailed accounting of all computer evidence is required. The search and seizure evidence log should include brief descriptions of all computers, devices or media located during the search for evidence. The log should document the date and time of the investigation, the names of all people who are involved with investigative activities (including witnesses and assistants to the search) and the location and a brief description of all computers, devices, and media. The investigators should make a note of these locations on the crime scene sketch as well.

Step 2: Document Computers, Devices and Media

After the evidence log is started, the investigator should proceed to record the state of all computers, devices and media. For each component, the following steps documentation should take place, using the evidence log where necessary or appropriate:

Computers [1]

- Take photographs of:
 - the computer screen;
 - the front, back and sides of the computer;
 - the cables attached to the computer; and,
 - any peripherals attached to the computer;
- log whether the computer is on or off; and, if it is on, note in the log what it appears to be doing;
- log whether or not the computer is on a network; and,
- log the potential for loss of data due to outside threats (such as weather,

electrical, magnetic).

Devices

- Take photographs of:
 - the front, back and sides of the device;
 - and the cables attached to the device;
- log whether the device is on or off, and, if it is on, what it appears to be doing.

Media

- If necessary or desired, photograph any media such as floppy disks, CDs, magnetic tapes, etc.; log the storage capacities of media if possible.

Step 3: Determine Whether or Not to Power Down Computers

Based on Step 2, it needs to be determined whether or not conditions permit a given crime scene computer to be shut down. If the investigator can't determine this on his own, the computer should be left running and the investigator should locate an operator who is an expert on the given system before proceeding. An example of a computer that typically should not be powered off is a mainframe or server that supports an organization's critical operations. If a machine is to be shut down, the investigator should be aware that it may have information stored on a RAM drive. In this case, steps should be taken to back up the RAM drive before proceeding. The assessment, and any actions taken in light of the assessment, should be noted in the search and seizure evidence log.

Step 4: Power Down Running Computers

The investigator should perform graceful shutdowns on the machines in question. This means he should use the normal shutdown procedures for a given computer's operating system. If a graceful shutdown is not possible (e.g., the computer is in a crashed state, the investigator is unable to become root, etc.), it should be determined whether or not an abrupt halt will cause too much damage to the computer's file system. If not, the computer should simply be turned off. Otherwise, the investigator will have to locate an operator who is an expert on the given system before proceeding. As always, all actions should be entered into the search and seizure evidence log.

Step 5: Mark and Tag All Hardware, Cables and Media

Wire tags and stick-on labels should be used to identify computers and devices (and cables belonging to each). Stick-on labels can also be used to identify media. If there is more than one computer at the crime scene, the investigator should employ a lettering/numbering system to distinguish each computer's peripherals and cables. It may be convenient to perform this step as evidence is located during the initial search.

Step 6: Prepare Computers, Devices and Media for Transport

All computer evidence needs to be readied carefully for transport to an evidence preservation lab. The investigator should package computer cables, and hardware in sturdy, cardboard boxes, labeling the boxes with their contents. Packing foam and anti-static plastic covers should be used whenever possible, and storage media should be placed into appropriate containers (e. g., diskette, CD, or tape storage containers). All boxes belonging to a given computer system should be kept together to make loading and unloading easier to track. As boxes are loaded for transport, another log file called the shipping manifest is used to record information that will be used later on to verify the delivery of all items at the destination. This information should include: date and time of shipping, contents of each box and name, or other identifier, of the person loading the boxes.

The investigator should be careful to keep all hardware and software away from excessive heat, and magnetic fields (a compass may be used to test for magnetic fields).

Step 7: Transport Computers, Devices and Media

Naturally, the investigator should be cautious about how the crime scene evidence is transported. While having it shipped by a commercial carrier or the U.S. Postal Service may be convenient, such means of transport can create a situation where the chain of custody is in question (e.g., after the evidence is dropped off at the shipper's depot, there is no reliable way to know who touched it and what they might have done to it during shipment). The ideal arrangement is one where the investigator himself transports the evidence back to the evidence preservation lab. In either case, the shipping manifest will provide a way to account for the evidence, when the evidence arrives at the lab.

Step 8: Unload Computers, Devices and Media

Upon arrival at the evidence preservation lab, all computers, devices and media from the crime scene should be carefully unloaded. The lead investigator or lab administrator should check off the items on the shipping manifest as they are moved. Simultaneously, each manifest entry should note the date and time of arrival and the name and initials (or some other identifier) of the person in charge of unloading.

All packages should be briefly inspected to verify that no tampering took place during transport. All evidence should be placed in the evidence preservation lab for safe keeping and detailed examination. The search and seizure evidence log and shipping manifest should also be stored in the lab when unloading is complete (note that with good case management software, all forensics logs will always be stored together in a secure, electronic manner).

Having examined the eight steps in evidence retrieval, we can now move on to discuss the final stage of the search and seizure process, processing computer crime scene evidence.

Processing Computer Crime Scene Evidence

| | | | | | |
|-----------------------|--|------------------------------------|----------------------------|--------------------------|-------------------------|
| (A) | (B) | (C) | (D) | (E) | (F) |
| Formulate plan | Approach and Secure Crime Scene | Document Crime Scene Layout | Search for Evidence | Retrieve Evidence | Process Evidence |

Figure 2: Processing Evidence - Stage F of a Search and Seizure

After being successfully transported to the evidence preservation lab, each piece of crime scene evidence must go through an initial accounting process. This helps to ensure the chain of custody, and properly introduces the evidence into the lab environment. This process includes the following steps:

1. start the lab evidence log;
2. mathematically authenticate the data on all crime scene computer hard drives and media;

3. generate bit stream backups of all crime scene computer hard drives and media prior to any forensic examination; and,
4. proceed with the forensic examination.

We will now examine each of these four steps in more depth.

Step 1: Start the Lab Evidence Log

The investigator should check all computers, devices, and media into the evidence preservation lab by starting a new lab evidence log (to be kept exclusively within the lab unless a decent case management program is being used). For each piece of evidence the following must be noted:

- date and time of arrival at the evidence preservation lab;
- a brief description of the evidence (should be the same as the description recorded earlier in the search and seizure evidence log);
- the condition of the evidence upon arrival (hopefully the same as what was recorded earlier!); and,
- name of the investigator checking in the evidence (may or may not be the same person who seized the evidence).

From this point onward, anyone wishing to interact with evidence must check the evidence out, and then check it back in when finished. Such an action includes the logging of the following items in the lab evidence log:

- date and time of check-out of evidence;
- identification of the evidence;
- name of the investigator checking the evidence out; and,
- date and time of when the evidence is checked back in.

Step 2: Mathematically Authenticate the Data

A utility such as GNU's md5sum (a freely available implementation of the MD5 hashing algorithm found with most distributions of Linux) is useful for generating a digital fingerprint for files. It is important to be able to prove that no alteration of electronic evidence took place after the evidence came into the investigator's possession. The md5sum utility generates a 128-bit message digest of its input; this can be anything from a file to an entire file system. According to MD5's creator, Ronald L. Rivest of MIT's Laboratory for Computer Science: "it is conjectured that the difficulty of coming up with two messages having the same message digest is on the

order of 264 operations, and that the difficulty of coming up with any message having a given message digest is on the order of 2¹²⁸ operations" [2]. Hence, md5sum is an excellent means to prove the authenticity of forensic evidence. The investigator should proceed in the following manner. First, the MD5 message digests for all original crime scene computer hard drives and media are generated, then all digests are recorded in the lab evidence log file.

When forensic work is complete, digest values are generated using the bit stream backups that were subjected to the forensic work. These values are then logged along side those from step 1. If the new values match the originals, it is reasonable to conclude that no evidence tampering took place during the forensic examination.

Since one of our overriding goals is to minimize interactions with original evidence (to ensure the integrity of that evidence), it's recommended that the investigator generate the initial MD5 digests when bit stream backups (see the next step) are generated.

Step 3: Backup all Crime Scene Computer Hard Drives and Media

As much as possible, forensic activities should be backed-up on bit stream backups of crime scene computer hard drives and media. Such backups are bit-for-bit copies of hard drive and media resources - meaning that all hidden, swap, deleted and normal file system data are included in the backups. By placing a bit-stream backup into a single data file (e.g., generated by the GNU dd program), it becomes trivial for the investigator to search the contents of the entire backup for strings of characters (e.g., with the UNIX strings command).

There are two ways to generate hard drive bit-stream backups. First, the computer can be booted in a controlled fashion from a boot diskette or CD and backed-up to some other device. Alternately, after the computer is shut down, its hard drives can be removed and duplicated in an evidence preservation lab machine or in a drive duplicator. The appeal of the first method is that there is no need to interact with the crime scene computer's hardware configuration. In fact, in some circumstances leaving the hardware untouched might be a necessity. The drawback, of course, is that the investigator ends up having to interact with the computer by running software on it to generate a backup. In contrast, the appeal of the second method is that the crime scene computer is not used (although its hard drives will ultimately be read). Instead, the hard drives are retrieved from the computer. Naturally, the drawback to this method is that the investigator must be sufficiently competent technically to remove and install

the crime scene computer hard drives. Either way, the bit stream backups must be obtained with as little destructive interaction as possible.

Creating backups for diskettes, tapes, CDs and other media are concerned is somewhat easier than for hard drives. These media are simply read, and their data are stored in a convenient location (i.e., hard drive, diskette, tape, CD, etc.). There is, of course, an expectation that the evidence preservation lab will have the devices necessary to read the various media in question.

Step 4: Proceed with the Forensic Examination

Using the bit stream backups from Step 3, the investigator may safely perform a forensic examination. Care should be taken to follow the basic rules of thumb given in [Search and Seizure Basics](#), as well as the Virus Protocol from [Search and Seizure: Approach, Documentation, and Location](#). All forensic work should be carefully logged in the lab evidence log. Each log entry should include the date and time of the forensic examination, a description of the forensic examination, and the name of the investigator.

Next Time...

In this installment of "The Field Guide for Investigating Computer Crime", we've wrapped up our look at search and seizure with a discussion of the retrieval and processing of computer crime scene evidence. Although the steps employed in both of these activities are quite involved, keep in mind that their overall aim is to ensure the chain of custody, and provide valuable documentation. Finally, good case management software can go a long way in easing the burden of carrying out a search and seizure.

The next article in this series will serve as a point of departure into information discovery. Recall that whereas search and seizure deals with physical computer evidence, information discovery involves only logical evidence (i.e., data). Despite this important distinction, we'll see many similarities between these two endeavors.

To read **The Field Guide for Investigating Computer Crime, Part 7: Information Discovery - Basics and Planning**, click [here](#).

References

- [1] Clark, Franklin and Diliberto, Ken. "Investigating Computer Crime," CRC Press, New York, 1996: pp 65-66.
- [2] Rivest, Ronald L. "RFC 1321: The MD5 Message-Digest Algorithm," MIT Laboratory for Computer Science, 1992. Found on the web at <http://www.andrew2.andrew.cmu.edu/rfc/rfc1321.html>.

For the past several years, Timothy Wright has been investigating computer fraud and abuse as a Senior Technology Investigator at one of the country's largest financial corporations. Before then, he worked as a lead developer within the financial industry, designing and building web-based home banking software. He holds an M.S. in Computer Science, and a B.A. in Philosophy.

Relevant Links

[Subscribe to the FOCUS-Incident Handling Mailing List](#)
SecurityFocus.com

[An Introduction to the Field Guide for Investigating Computer Crime](#)
Timothy E. Wright

[The Field Guide for Investigating Computer Crime Part 2: Overview of a Methodology for the Application of Computer Forensics](#)
Timothy E. Wright

[The Field Guide for Investigating Computer Crime Part 3: Search and Seizure Basics](#)
Timothy E. Wright

[The Field Guide for Investigating Computer Crime Part 4: Search and Seizure Planning](#)
Timothy E. Wright

[The Field Guide for Investigating Computer Crime Part 5: Search and Seizure Approach, Documentation, and Location](#)
Timothy E. Wright

[Privacy Statement](#)

Copyright 2006, SecurityFocus