

## Field Guide Part Three

*Timothy Wright* 2000-07-28

### In Our Previous Episode...

Previously, in [Overview of a Methodology for the Application of Computer Forensics](#) we took a high level tour of a formal, methodical process for investigating computer crime. Our tour consisted of an overview of the two endeavors which comprise this process: search and seizure, and information discovery. Along the way, we considered why a formal method for investigating computer crime is truly necessary, and we related our method back to the well-known scientific method. Now, we're ready to take the plunge into the gritty details of the search and seizure forensic activity. However, a word of warning is in order: things become reasonably involved from this point on; try not to get overwhelmed. Keep in mind that the degree of complexity in the search and seizure process can always be scaled back in accordance with an organization's investigation policies (e.g., high profile cases are given the full treatment, low profile cases are given a less involved treatment).

To begin our discussion of search and seizure, it's crucial that we establish a common sense foundation; that is, a few simple, yet important, guidelines. These will serve to steer an investigator's search and seizure operations away from some of the more common pitfalls.

### The Basic Rules for Search and Seizure

As mentioned in [Overview of a Methodology for the Application of Computer Forensics](#), search and seizure involves the recovering and processing of physical computer evidence from a computer crime scene. Although mostly just good, common sense, the following six rules should always be in the mind of the investigator throughout the stages of search and seizure forensic work:

1. Do not alter original evidence [1, pg. 3]
2. Do not execute programs on a crime scene computer (especially the operating system)
3. Do not allow a suspect to interact with a crime scene computer [1, pg. 3]
4. Always back up a crime scene computer; if a crime scene computer is on, do not turn it off until any valuable data in temporary memory have been saved
5. Document all investigative activities
6. Regarding the storage of computer evidence: if you are comfortable there, then the

computer and components will be comfortable there [1, pg. 37]

In particular, these rules of thumb are helpful for establishing a protocol by which evidence is accounted for, gathered, handled and stored. Not only is this essential for tracking and managing evidence that may originate from a computer crime scene, but such a protocol also protects against "...a defense attorney [who] wants to get your evidence thrown out of court because of potential mishandling" [1, pg. 26]. Further consideration is now given to each of these six rules.

**Rule 1: Do Not Alter Original Evidence** It is an easy task to keep from altering hardware and software evidence when that evidence is not in use (e.g., powered down, not running, etc.). However, when a computer is running, it becomes largely impossible to keep from changing its physical and logical state during interactions. In fact, even when an operational computer sits unattended it might be busy writing to I/O buffers, executing timed jobs, and performing any number of housekeeping chores. Even simple operating systems can have TSR (terminate and stay resident) programs executing in the background. Realistically, any interaction a user has with a running computer can cause changes in that computer's state. Whenever a user so much as makes a keystroke at the keyboard, changes are enacted in the disposition of the computer. Such changes can have dire effects on potential electronic evidence.

With running hardware and software systems, great care must be taken by the investigator to minimize all interactions, thereby diminishing the potential for alterations to these systems.

This means two things:

- A. During any direct examination of a crime scene computer, a boot diskette or boot CD should be used if the computer is to be powered on (obviously mainframe computers will not be accessible in this manner). Ideally, such examinations should be refrained from; see the following point.
- B. As much as possible, forensic activities should be performed on the bit stream backups<sup>1</sup> of crime scene computers (and storage media) - this follows from the fourth rule of thumb listed above.

By booting a computer from diskette or CD, some of the activities associated with a normal hard disk boot strap are circumvented. Even with this measure of safety, however, it is always best to interact with bit stream backups of crime scene computers to ensure that original evidence is not altered. Unfortunately, in order to get a bit stream backup of a system, that

system has to be interacted with at some level; this will be addressed more completely in a future installment of the field guide. Additionally, some operating systems are better suited than others to forensic work. As mentioned in the introduction to this guide, Linux is a highly robust, stable and secure POSIX operating system, offering significant support for different computing environments. Because Linux also happens to be able to fit on one or two diskettes (depending on the configuration), it makes for an excellent investigative tool. For example, an investigator might wish to put together a diskette distribution of Linux with support for IDE and SCSI drives, networking, and some basic file system utilities. If more capacity is needed, Linux can also be installed to run off of a ZIP or JAZZ cartridge (see, for example, the [Trinux](#) and [tomsrtbt](#) web sites).

**Rule 2: Do Not Execute Programs on a Crime Scene Computer** In general, crime scene computers should be viewed as museum exhibits: look, but do not touch. Executing any program directly on such a computer could cause damage to valuable electronic evidence, or, at the very least, change the state of various computer resources (e.g., memory, swap files, the file system in general, etc.). Because of its housekeeping abilities, a computer's operating system has enormous potential for causing such damage (e.g., valuable temporary and cache data could be "cleaned" out of existence). For those rare exceptions when software must be executed on a crime scene computer, extreme caution should be used and all activities should be carefully documented.

**Rule 3: Do Not Allow a Suspect to Interact with a Crime Scene Computer** Electronic evidence will disappear quickly at the hands of a suspect. There should never be any reason to allow a suspect to interact with a crime scene computer or computer component!

**Rule 4: Always Back Up a Crime Scene Computer** Bit stream backups of crime scene computers are essential to forensic work: investigative activities should be limited to backups to ensure the integrity of original evidence. An interesting matter related to the backups of computers, is the RAM drive. An investigator should consider whether or not an operating crime scene computer has a drive or drives implemented in resident memory. Obviously, the bit stream backup of such a drive requires interacting with the computer's operating system - something that goes against both the first and second rules of thumb defined above. However, a RAM drive could prove to be an invaluable store of evidence. Extreme caution and the investigator's common sense should be used here.

**Rule 5: Document all Investigative Activities** Documentation is of the utmost importance

during all computer forensics work. From the moment a case is opened, to the moment it is closed everything an investigation involves should be carefully logged along with a time and date. One way to implement logging, is for the investigator to use a notebook or sub-notebook computer with a simple spreadsheet program. With this, whether work is being done in the field or the evidence preservation lab, proper documentation can be kept. Of course, certain precautions with such a setup have to be taken: the spreadsheet data should be stored in a password protected, encrypted format, and should be backed up at reasonable intervals. Note that the investigator should keep separate spreadsheets for field and lab work. **A better alternative to using spreadsheets would be to use case management software!** As outlined in our previous installment ([Overview of a Methodology for the Application of Computer Forensics](#)) an investigator risks having a weaker chain of custody and little control over a case's information without good case management software.

**Rule 6: The Storage of Computer Evidence** While it is generally true that hardware and software evidence can be physically well cared for in environments that are also comfortable to humans, the investigator should be wary of electromagnetic fields, static electricity and dust. To reduce the transmission of static charges, Clark and Diliberto recommend the use of wood shelves and cabinets for storage whenever possible [1, pg. 37].

Based on the description of Rule 4, regarding the need to create backups, it appears as though there is a measure of contradiction built into these rules of thumb. A more detailed treatment of backups will be given in a future installment, but the topic is important enough to warrant some discussion at this juncture. The crux of the problem is this: an investigator often comes across situations where it is impossible to keep from interacting with a running computer; but such interactions, as we know, can have destructive consequences on the original state of computer evidence. What, then, can an investigator do to prevent this? For example, what steps should an investigator take when faced with a running computer which must be shut down in order to be transported to an evidence preservation lab? The act of gracefully or non-gracefully powering a workstation down can result in significant and permanent changes to a file system, executing processes, and, of course, memory. Any of these things can hold vital clues for an investigation. And what about RAM drives? Although touched on in the description for Rule 4, nothing definitive was really offered by way of a protocol for dealing with memory data stores. There is an adage that seems appropriate here: in theory, theory and practice are the same; in practice, they are not. Although an investigator has every intention of avoiding all destructive interactions with a crime scene computer, the truth of the matter is that many times this is impossible. When dealing with the possibility of a RAM drive, an investigator must assess

whether the importance of finding and backing up that drive outweighs the destructive changes such activities will cause to the crime scene computer. When dealing with the prospects of having to power down a workstation in order to transport it to an evidence preservation lab, the same evaluation must be made. The best that an investigator can do is to thoroughly document the crime scene computer's original state, along with the steps taken during interactions, and be as careful and conservative as possible in these interactions.

## Next Time...

In this installment of The Field Guide for Investigating Computer Crime, we've taken the first step into the process of search and seizure. This entailed a discussion of six fundamental rules to guide an investigator during a search and seizure. In essence, these rules are devised to help prevent the mishandling of evidence, and encourage the documentation of search and seizure activities. In other words, the rules help to ensure an investigation's chain of custody, which is critical to the success of any case.

In our next article, we'll examine the planning stage that must take place prior to any investigator arriving at the computer crime scene, including two ways to structure a team of investigators. In future articles we'll then turn our attention to the remaining stages of search and seizure, and head on into the process of information discovery.

To read **The Field Guide for Investigating Computer Crime: Search and Seizure Planning (Part 4)**, click [here](#).

## References

(1) Clark, Franklin and Diliberto, Ken. "Investigating Computer Crime," CRC Press, New York, 1996.

(2) Saferstein, Richard. "Criminalistics: An Introduction to Forensic Science, Sixth Edition," Prentice Hall, Upper Saddle River, New Jersey, 1998.

<sup>1</sup> A bit stream backup is an exact copy of a file system which includes every last bit of data belonging to normal, hidden, or deleted files.

<sup>2</sup> This can also destroy the chain of custody.

*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

[An Introduction to the Field Guide for Investigating Computer Crime Part One](#)

*Timothy Wright*

[The Field Guide for Investigating Computer Crime Part Two: Overview of a Methodology for the Application of Computer Forensics](#)

*Timothy Wright*

[Privacy Statement](#)

Copyright 2006, SecurityFocus