

## Field Guide Part Two

*Timothy E. Wright* 2000-05-26

### In Our Previous Episode...

Previously, in [An Introduction to the Field Guide for Investigating Computer Crime](#), we considered the basics of computer crime and computer forensics. We began with a definition for computer fraud and abuse, then discussed evidence and the importance of chain of custody, and finished up with an outline of the skills and tools needed to investigate computer crime. With all of that behind us, we can turn our sights toward the heart of the matter: a methodology for investigating computer crime.

### The Methodology At a Glance

Our methodology is comprised of two similar, yet distinguishable parts: search and seizure, and information discovery. These two broad areas of forensic work can be best viewed as the physical, and the logical. In search and seizure, the investigator is dispatched to a computer crime scene, and faces the task of recovering and processing physical evidence. By contrast, information discovery involves the investigator accessing data sources on un-seized materials (e.g., log files, databases, etc.), in an effort to locate and process information that may prove or disprove something. Often, a case may require search and seizure as well as information discovery.

Figures 1 and 2 provide a high level road map of the stages involved in the search and seizure, and information discovery processes (we refer to stages within these processes; eventually we'll see that each stage is comprised of individual steps).

| (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: High Level Stages for a Search and Seizure**

|                              |                                   |                                |
|------------------------------|-----------------------------------|--------------------------------|
| <b>(A)</b><br>Formulate Plan | <b>(B)</b><br>Search for Evidence | <b>(C)</b><br>Process Evidence |
|------------------------------|-----------------------------------|--------------------------------|

**Figure 2: High Level Stages for an Information Discovery**

A quick glance at both figures reveals that while there are stages in common, Figure 1 is much more involved. This is because search and seizure deals with physical evidence such as computers, components, and media, as opposed to the logical evidence of information discovery. Finding, documenting, and retrieving physical evidence can be an especially difficult task since care must be taken in managing a crime scene and handling evidence found there. Logical evidence, on the other hand, doesn't present as many issues because it is in an electronic format. One might be tempted to assume that information discovery necessarily follows the stages for search and seizure: e.g., after locating a computer at a crime scene, an investigator performs information discovery activities on that computer to look for logical evidence on its hard drive. Although sound in concept, this is incorrect in practice. The last stage of search and seizure, *Process Evidence*, is where an investigator would actually examine the data on a crime scene computer's hard drive. The distinguishing characteristic here is that information discovery does not take place on seized computers, components, or media. Rather, it is the retrieval of logical evidence on un-seized materials. Throughout any forensics processes, of course, the investigator must be careful to document his or her steps, and preserve the chain of custody. Let's briefly consider figures 1 and 2 more closely.

The process of search and seizure is comprised of many stages, and, frankly, is quite tedious. It begins with Stage A, Formulate Plan, wherein the lead investigator sizes up the task at hand, determines what evidence is being looked for, and decides how the search for evidence will proceed. Roles and responsibilities are assigned to other investigators at this point. In Stage B, *Approach and Secure Crime Scene*, the investigators arrive at the crime scene and secure its premises from unauthorized people. Stage C, *Document Crime Scene Layout*, involves an investigator carefully noting where relevant items and evidence are located within the crime scene. Stages D and E, *Search for Evidence* and *Retrieve Evidence*, respectively, have investigators finding, packing up, and moving evidence (to an evidence preservation lab). Finally, Stage F, *Process Evidence*, involves the management and analysis of evidence within an evidence preservation lab.

In contrast to search and seizure, the process of information discovery is quite simplistic. Here, Stage A, Formulate Plan, is similar to the same stage in search and seizure. Stage B, Search for

Evidence, involves an investigator accessing data repositories (e.g., log files, databases, the Internet, etc.) in an effort to locate information relevant to a case. Lastly, Stage C, Process Evidence, is similar to Stage F in search and seizure.

The ability of an investigator to securely (e.g., chain of custody, etc.) and efficiently manage computer evidence and case data is the corner stone of this methodology. The field guide introduction touched on this during its discussion of what a case management system is. The most sound and expeditious means of tracking evidence and handling case data, is to use a software system designed for that purpose. However, in the absence of money to buy, or the wherewithal to build such a system, the investigator can turn to other, less potent options. For example, a spreadsheet or word processor can be used to create case note templates that can be filled in with appropriate information during an investigation. Naturally, such hacks will need to be secured in some fashion in order to mitigate the chance of an unauthorized person from obtaining or tampering with sensitive case information. Encryption software such as [PGP](#), provides an easy means for securing the likes of spreadsheet, and word processor documents.

Taking notes on paper, is also a possibility here, but not without a few unfortunate drawbacks. First, hand written notes can't be secured as easily as electronic files. Second, hand written notes can't be integrated into other sources of information as conveniently as electronic files can be integrated with electronic sources of information. And third, hand written notes can't be readily stored in computer databases for searching and analysis. This isn't to suggest that investigators should avoid writing things down on paper. Instead, case data should be collected into a secure electronic format as soon as possible. Ideally, an investigator will be able to write his or her notes directly into a case management system so that these data are protected and made available to a database of case information. Not-so-ideally, an investigator can record notes in a spreadsheet, word processing document, or on paper - hopefully at some point entering these notes into a database of some sort.

## **This thing is a pain in my backside! Why do I need a formal methodology, anyway?!**

Indeed, there is no question that using a formal methodology to carry out computer fraud and abuse investigations requires some effort. However, there are compelling reasons to do so. A formal methodology allows an investigator to approach and investigate a computer crime rationally and expeditiously, without a loss of thoroughness. More importantly, it establishes a protocol by which electronic evidence (physical and logical) is gathered and handled, to reduce

the potential for this evidence to be corrupted or tainted. Without such a methodology, it will be more difficult to successfully investigate, and, therefore, control computer fraud and abuse. An inability to resolve such incidents will end up costing our computing society more and more money each year.

Beyond even this strong line of reasoning, the core of any forensic science (computer related or not) is, of course, science! It is, therefore, requisite that any investigative processes used to carry out computer forensics, also exhibit the characteristics of a scientific methodology. For example, a valid process should consist of rational, well-conceived steps that can be repeated in all investigations. In addition, such steps should help safeguard against inconsistent and biased results, by providing a framework of reason within which investigative activities can take place. Without a formal, well-practiced methodology, an investigator is really just "doing stuff" in a non-scientific, ad hoc manner. Evidence compiled by investigators who just "do stuff" is not taken too seriously in courts of law.

Before leaving the topic of scientific methodologies and investigative processes, a brief outline of the generic scientific method itself might prove useful.

1. Identify and research a problem
2. Formulate a hypothesis
3. Conceptually and empirically test the hypothesis
4. Evaluate the hypothesis with regards to the test results - devise and execute new tests if the results are inconclusive
5. If the hypothesis is acceptable, evaluate its impact

It's interesting to note how we can apply the scientific method at all levels of the computer forensics endeavor. For example, at a very high level, we find that step 1 of the scientific method takes place when a crime has been committed and brought to the attention of an investigator; step 2 corresponds to the investigator considering the "who-what-where-when-why-how" questions related to the crime; steps 3 and 4 make up the process of gathering and evaluating evidence in support of a hypothesis devised in step 2; and step 5 denotes the conclusive activities that happen when an investigation is completed. At a more detailed level, these steps are applied over and over during the *Process Evidence* stages within search and seizure, and information discovery.

## **Scope of Application for the Methodology**

Faced with some of this methodology's intricacies, it's natural to ponder whether or not all of the various steps need to be applied in all investigations. The theoretical answer to this is yes. If an investigator doesn't apply all of the steps in all of his or her investigations, then a loss of parity will occur amongst case data - with some of these data being more thorough and complete than others. Such a loss of parity can introduce weaknesses into evidence that an investigator might have to present in court (e.g., weaknesses not only in the evidence itself, but also in the procedures used by the investigator to gather the evidence). On the other hand, the practical answer to this question is: it depends on how much risk an investigator (or an organization) is willing to take. Deploying a formal method for investigating computer crime is obviously resource intensive. By selectively using the method in its entirety on only high profile cases, the process of investigation can be streamlined. However, the risk, as pointed out above, is that serious weaknesses can be introduced into evidence gathered by an investigator.

It's worth mentioning that a possible solution to the issue raised above might be as follows. The processes of search and seizure, and information discovery could be different for different categories of urgency assigned to a case. Within each category, however, these processes would be carried out in exactly the same way. Hence, for the most important cases, say, category 1 cases, all of the steps outlined in the previous section would be carried out for search and seizure, information discovery, or both. For slightly less important cases, category 2, streamlined versions of search and seizure, and information discovery would be deployed. This tactic is different than an investigator applying our formal methodology in an ad hoc way for each case worked. Instead, the formal methodology is amended to specify that for cases of low priority (e.g., category 2) a streamlined version of search and seizure, and information discovery is used. This is a very important distinction, in that it means that there is an established policy for knowing when to apply which version of the formal methodology.

## **Next Time...**

In this installment of the Field Guide for Investigating Computer Crime, we were presented with an overview of our formal methodology for investigating computer fraud and abuse. We found that this methodology is broken up into two processes: search and seizure (for physical computer evidence), and information discovery (for logical computer evidence). Also, we looked at why using a formal methodology for computer crime investigation is so important, and what the consequences might be if such a methodology isn't adhered to in all investigations.

In our next installment, we'll dig into the details behind the search and seizure process. We'll see that this is the most involving and difficult activities an investigator can undertake. Then, in our final installment, we'll take a hard look at information discovery.

To read **The Field Guide for Investigating Computer Crime: Search and Seizure Basics Part 3**, click [here](#).

*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*

[CCIPS](#)

*Department of Justice*

[Zeno's Forensics Page](#)

*Zeno*

[Reddy's Forensics Homepage](#)

*Reddy*

[Privacy Statement](#)

Copyright 2006, SecurityFocus