

Field Guide Part Seven

Timothy E. Wright 2001-02-26

The Field Guide for Investigating Computer Crime, Part Seven: Information Discovery - Basics and Planning

by *Timothy E. Wright*

last updated Feb. 26, 2001

Last Time...

Earlier in the Field Guide for Investigating Computer Crime, we outlined the two major parts of our investigative methodology: search and seizure, and information discovery (for more the details, please see [Overview of a Methodology for the Application of Computer Forensics](#)). The previous installment in this series, [Search and Seizure, Evidence Retrieval and Processing](#), concluded the overview of search and seizure with a discussion of the retrieval and processing of computer crime scene evidence. In this installment of the Field Guide for Investigating Computer Crime, we will begin our discussion of information discovery, the process of viewing log files, databases, and other data sources on unseized equipment, in order to find and analyze information that may be of importance to a computer crime investigation.

Information Discovery: An Introduction

The search and seizure process is concerned entirely with physical computer crime scene evidence: an investigator goes to a computer crime scene, secures it, searches for evidence, and brings that evidence back to a lab where it is processed. Information discovery, on the other hand, deals with logical, which is to say electronic data, evidence. Some objectives of information discovery might include:

- Verifying whether or not a user of some computer system has exceeded or abused his access privileges
- Determining whether or not a particular system transaction took place within a given period of time, and who (or what) enacted that transaction
- Accounting for the activities of a user or group of users on a computer system within a given period of time
- Tracking an e-mail message back to its source (e.g., e-mail stalkers, spam mail, nuisance mail)

The Basic Rules for Information Discovery

The objectives of information discovery may include not stand-alone systems, but entire networks of computers. In fact, the information discovery process may frequently take place on corporate intranets as well as on the Internet. Regardless of where this process is carried out, as with search and seizure, there are certain fundamental rules that the investigator must follow. For those readers who have been following this series so far, many of these rules may seem familiar, that is because many of the procedures that apply to search and seizure operations are also relevant to information discovery. Some of the basic rules for information discovery include:

1. Do not alter discovered information;
2. Always back up discovered information;
3. Document all investigative activities.

Each of these rules is examined below.

Rule 1: Do Not Alter Discovered Information

It is imperative that the investigator not alter recovered evidence in the course of forensic activities. Hardware-based and software-based evidence may be altered in the course of investigation, since, somewhere along the line, hardware may have to be powered up, and software may have to be executed. However, in information discovery, these risks are mitigated since information can neither be powered on nor executed. Still, the investigator must avoid doing anything that would alter discovered information (e.g. destructive writes). One easy way to ensure this is to store information within read-only files. A safer and more reliable method is to use a revision control system, which we will discuss in the next instalment of this series. In either case, the investigator should always create a message digest of the discovered information, to be able to show that these data have not been altered during the course of investigation.

Rule 2: Always Back Up Discovered Information

While the investigator should, as much as possible, minimise all direct interactions with computer crime scene evidence, the evidence must somehow be preserved. The best way to preserve evidence is by backing it up, so that all forensic activities can be performed on bit stream copies instead of the original evidence, which needs to be maintained. Destructive interactions with an original information file can be avoided by backing up the file immediately

after its creation (that is, immediately after the investigator gathers evidentiary data into a file). As suggested in Rule 1, a revision control system can be an excellent way to maintain backups of files while at the same time ensuring their integrity (e.g. all interactions are carried out with copies of the original files, and an audit trail is maintained).

Rule 3: Document All Investigative Activities

Documentation is critical in all computer forensics work, and must be maintained from the opening to the closing of a given case. All investigative activities should be consistently described and logged with a time and date stamp. A simple spreadsheet program can provide a convenient way to implement logging, but case management software, with built in security and convenience, is preferred. If a spreadsheet is used, its data should be stored in a password protected, encrypted format, and should be backed up at reasonable intervals.

Information Discovery Stage A: Planning

(A)	(B)	(C)
Formulate plan	Search For Evidence	Process Evidence

Figure 1: Planning - Stage A of an Information Discovery

Even though information discovery does not deal with the search for, or collection of, physical evidence (e.g., hardware and computer media), the steps for planning the discovery process are similar to the steps for planning a search and seizure. In fact, the only real difference is that there is not a computer search team to carry out information discovery; rather, under normal conditions, one person can do this job adequately, especially with the help of simple automated search tools (e.g. batch processing utilities, scripts, etc.)

It is important to have a carefully considered plan of attack before launching into the actual information discovery. This will ensure that the investigator possesses a clear understanding of what he is looking for and will minimize the risk that target information will be destroyed or contaminated during its retrieval. The following describes four steps, which are also described in Search and Seizure Planning are required in the planning of information discovery:

1. accumulate the computer hardware and storage media necessary for the search circumstances;
2. prepare the electronic means needed to document the search;
3. ensure that specialists are aware of the overall forms of information evidence that are expected to be encountered as well as the proper handling of this information;
4. Evaluate the current legal ramifications of information discovery searches.

Some brief points need to be made about each of these steps.

1: Accumulate the Computer Hardware and Storage Media Necessary

Given the importance that we have placed on backing up electronic evidence, this first step is crucial. Data found during an information discovery may turn out to be volatile (i.e., after a certain duration of time, they may be deleted, written over, or changed in some way); if the investigator does not have enough media to store this data, he may end up losing it entirely. One can not have too much of a computing resource - it is far better to end up with ten unused JAZZ cartridges and all of the discovered information, than two full JAZZ cartridges with only some of the discovered information.

2: Prepare the Electronic Means Needed to Document the Search

In order to maintain the integrity of the investigation, it is necessary to document all aspects of the information. This step can be implemented with a spreadsheet program, or some other relevant form of electronic documentation (which, ideally, is maintained in a password protected, encrypted format) such as case management software. Having the necessary means for documentation ready prepared beforehand, will save time and confusion during the information discovery process.

Two logs in particular will be needed: a information discovery evidence log, and a lab evidence log. The information discovery log will allow the investigator to track data regarding all information files found during the information discovery process. The lab evidence log provides a way to track data about the information files as they are forensically examined. We'll discuss these log files further in the next installment of our field guide.

3: Ensure That Specialists Are Aware of the Overall Forms of Information Evidence Expected

Similar to the third step in Search and Seizure Planning, preparatory work for information discovery must include a consideration of what data (i.e., their morphology and semantic value) are being sought and how best to conduct a search for them. With this preparation, the investigator can avoid aimlessly sifting through data repositories by tailoring his search strategy to fit the target information. Also, the possibility of contaminating the information evidence (by the very act of searching) can be minimized. For example, an investigator may need to check the shell history file for a suspect's UNIX account; however, logging in as the suspect is a poor way to go about doing this, as it will cause new activities not committed by the suspect to be written into the history file, thereby contaminating it.

4: Evaluate the Current Legal Ramifications of Information Discovery Searches

Finally, as with a search and seizure, the investigator must always be cognizant of the rights of suspects, particularly their privacy rights! In particular, where information discovery is concerned, special attention needs to be paid to the [Electronic Communications Privacy Act](#) to ensure that the investigation is conducted in a legal and ethical manner. In theory, corporate investigators should have no difficulty gathering information that is owned by their company. Nevertheless, they should always consult their legal department first, to verify what can and cannot be investigated and/or obtained.

Next Time...

In this installment of the Field Guide for Investigating Computer Crime, we began our consideration of the process of information discovery. The fact that information discovery only deals with logical evidence (i.e., electronic data), means that we can avoid much of the tedium required by search and seizure to ensure evidence integrity and the chain of custody. Nevertheless, as we have seen, there are strong similarities between the two processes throughout their respective basic rules and planning stages.

For information discovery, where the basics are concerned, the investigator is occupied with safe guarding the chain of custody. While during the planning stage, emphasis is given to understanding the information being sought after. Backups of discovered information files are

critical to the overall process, and tools such as revision control software can be very handy for this task.

In our next article, we'll outline the remaining stages of the discovery operation - the search for data evidence and processing discovered data. In fact, that will pretty much wrap things up for the field guide, so be sure not to miss it!

To read **The Field Guide for Investigating Computer Crime, Part Eight: Information Discovery - Searching and Processing**, 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

[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

[The Field Guide for Investigating Computer Crime, Part 6: Search and Seizure - Evidence Retrieval and Processing](#)
Timothy E. Wright



[Privacy Statement](#)
Copyright 2006, SecurityFocus