

## Field Guide Part One

*Timothy E. Wright* 2000-04-17

### Abstract

As computers and the Internet continue to pervade and invade our lives, the potential for harm caused by computer crime increases manifold. Unfortunately, there is a deficit of information about what computer crime is, and how it should be investigated. As a result, such criminal acts become more widespread and costly to our society each year. The relatively new field of Computer Forensics attempts to manage this problem by providing a thorough, efficient, and secure means of investigating computer crime. This article and those which follow, will endeavor to provide a field guide for the computer fraud and abuse investigator. In a plain and approachable manner, this guide will cover a generic method for the application of computer forensics. Beginning here with a discussion of the basics, the field guide will address questions and issues fundamental to investigating computer crime, and detail a method for doing search and seizures of physical computer evidence, and information discovery of logical computer evidence. For those readers who are not computer fraud and abuse investigators, it is hoped that common sense will be imparted about what and what not to do as the victim of a computer crime.

### Setting the Scene

It seems as though a wake-up call has been blasted at us from all corners of the Internet. Web sites are routinely defaced, denial of service attacks are more common, and e-commerce sites are broken into and plundered. But this is all just the tip of a very ponderous iceberg. For years now, information technology (IT) operations have been the silent victims of all manner of computer fraud and abuse from inside and out of their network borders. Incidents ranging from unauthorized accesses and malicious destruction of data, to logic bombs, hacking, and the disclosure of confidential information have been a scourge for those in IT. In a [computer crime survey](#) conducted annually by the Computer Security Institute and FBI, only 51% of 1999's survey respondents could (or would) acknowledge that they had suffered a financial loss due to computer crime. Even more alarming, only 31% of the respondents could put a dollar figure on their loss! Hence, the \$123,779,000 dollars reported by the survey as lost, is merely a lower bound for the survey's participants. This same survey [conducted for 2000](#) shows that 74% of the respondents acknowledged financial losses resulting from computer crime, and 42% reported losses of \$265,589,940. It's a good time to be a computer fraud and abuse

investigator!

A primary reason that the IT industry has difficulties in accounting for, and assessing the costs of computer crime is that there is very little good information about what computer crime is and how it can be investigated. In their White Paper on Computer Crime Statistics, the International Computer Security Association, points out that:

- Most computer crimes go undetected by their victims
- Of the attacks which are detected, few are reported

As a computing society, we are now presented with a situation that can profoundly increase the costs and risks of utilizing electronic, information services.

But what, exactly, is computer fraud and abuse? Computer fraud involves a criminal act, while computer abuse deals with violations of an organization's computer use policies. Where computer fraud is concerned, a perpetrator who violates [Title 18, Section 1030](#) of the U.S. Criminal Code can be sent to prison for many years, and heavily fined. In contrast, computer abuse can result in a reprimand, demotion, or termination of employment. By not knowing how to perform the task of investigating computer fraud and abuse, dealing with a potential computer crime becomes nearly impossible. Computer crime, in turn, becomes more dangerous and damaging. To address the task of investigating computer fraud and abuse, a relatively new field called Computer Forensics is emerging.

## Some Basics of Evidence

Computer forensics is concerned with the gathering and preserving of computer evidence, as well as the use of this evidence in legal proceedings (the focus of this field guide will be on evidence and not legal proceedings). For our purposes, such evidence is both physical and logical, in that it may consist of hardware components and media which contain data, or just data alone. The physical side of computer forensics involves what is called **search and seizure** of computer evidence. Here, an investigator travels to the scene of a computer crime, and searches for, and takes into custody computer hardware and media that are involved in the crime. In contrast, the logical side of computer forensics deals with the extraction of raw data from any relevant information resource. This is referred to as **information discovery** and normally involves an investigator combing through log files, searching the Internet, retrieving data from a database, etc.

There's a definitive issue that general forensics science grapples with concerning evidence. Namely, an investigator must be able to extract information from the evidence at hand, but without causing changes to the original state of this evidence. Furthermore, the original state of the evidence must be preserved throughout an investigation - from the moment the evidence is located, to the moment the investigation is closed (and, perhaps, thereafter!). The efficacy of evidence as objective documentation, depends on how well the evidence has been preserved. As we shall see, in the practice of computer forensics, there can be moments when ensuring the state of evidence is at best very difficult; sometimes, the alteration of even a few bits of data can have drastic consequences on an investigation.

An important tool used by investigators to safeguard evidence, is something called the **chain of custody**. Essentially, this is a means of accounting for who has touched a given piece of evidence, when they touched it, and what they did to the evidence. It's a way of demonstrating that evidence hasn't been damaged or tampered with while in the care of the investigator. In his book, *Criminalistics: An Introduction to Forensic Science*, Richard Saferstein notes, "Failure to substantiate the evidence's chain of custody may lead to serious questions regarding the authenticity and integrity of the evidence and the examinations rendered upon it (pg. 48)." As one would imagine, changes to the chain of custody can quickly ruin a case.

## The Right Tools for the Right Job

Computer forensics is unlike any other forensics activity: preserving and interacting with the evidence of a computer crime requires skills and tools drawn from both traditional forensics and computer science. As with other types of evidence, when mishandled, or managed with a weak chain of custody, computer evidence becomes useless. Beyond this, however, computer evidence is inherently complex and volatile in its own unique way. We find it to be complex because it can be derived from any computing resource, at any level of operation (e.g., machine language all the way up to meta-data and beyond). We also find it to be volatile, since it can be digitally altered or destroyed with ease, and often without detection. To cope with these issues, the skills and tools that the computer fraud and abuse investigator deploys must be tailored to fit the job. Let's consider skills followed by tools.

An effective computer fraud and abuse investigator must have a fundamental understanding of information systems - only being able to turn on a PC and use a word processor or web browser does not pass muster here. The investigator must be familiar with good systems administration

practices, and possess skills and knowledge relevant to computer security. He or she must understand how computers, operating systems, databases, and computer networks function, and must have a basic understanding of the various concepts at work in these areas (e.g., computer organization, distributed computing, database architecture and administration, network architecture and protocols, etc.). In addition to this extensive background of skills and knowledge, the effective computer fraud and abuse investigator must also have the imagination and deductive skills to solve cases!

The tools needed to investigate computer crime are relatively straight-forward, consisting of both hardware and software. First, on the hardware side, an evidence preservation lab is required. This is a highly secure environment (physically and logically) where computer evidence is processed and stored. It has physical accommodations to help an investigator perform a variety of tasks, as well as experiment and interact within a range of computing environments. Such a lab might include: ethernet and token ring LANs, Linux workstations, other UNIX workstations, PCs, tape backup systems, CD reader/writer systems, high capacity removable media drives, and a sufficient amount of fresh, blank media. To assist and enable the computer fraud and abuse investigator in the field, a decent notebook computer is desirable as well. There are times when an investigator's notebook has to be used in the capacity of a "lab away from the lab;" for example, to analyze or store data. Also, as we'll see below, a notebook is quite useful as a client for accessing a case management system.

Regarding the software tools needed for investigating computer crime, software to run the evidence preservation lab is requisite. This would include operating systems, database systems (e.g., for storing and analyzing case data), data archiving programs to manage the tape backup and CD reader/writer systems, and a case management system. The case management system is a key component in the investigative process, since it provides the investigator with a means of storing case notes and information about all of the players and items in a given investigation. The questions about "who," "what," "where," "when," and "how" are addressed for each case in the data stored by the case management system. Ideally, these data should be stored and interacted with in a secure manner: when case data are transmitted or archived they should be strongly encrypted, and access to case data should be through a means using strong authentication. Of course, the case management system should provide all of the expected features of any database, such as the ability to search on, and generate statistics for case data. A case management system also needs to be accessible outside of the evidence preservation lab. With this, when an investigator is in the field, he or she can (securely) retrieve, and work on case notes for an investigation. Further discussion about the case management system is

really outside of the scope of this field guide. Suffice it to say that any computer fraud and abuse investigator who operates without such a system is doing so at the peril of his or her work. This is because the case management system is instrumental in maintaining a strong chain of custody, and good organization.

One last software tool needs to be discussed: the GNU/Linux operating system (referred to as "Linux" hereafter). Throughout this guide, numerous references to Linux will be made regarding tools that can be used to facilitate computer forensics activities. Linux is a stable, secure, and efficient operating system. Well supported on the Intel, Sun, Alpha, PowerPC, and Motorola platforms, Linux adheres to the POSIX standard, offers kernel level threads and multiprocessor support, boasts an enormous software base, and, of course, is free. Perhaps the greatest feature of this beautiful operating system is its high standard of quality. This is due to the development philosophy that Linux employs: anyone who wishes may offer enhancements and additions to the Linux kernel, but all such changes are subject to the extensive review and critique of the Linux community. The end result is software in which Linux users maintain a high stake. This is especially important to the endeavor of computer forensics, because it means that Linux provides a relatively safe, robust and feature rich platform upon which to work. Having Linux installed in the evidence preservation lab, as well as on the investigator's notebook is an excellent way to have access to some invaluable software utilities (thanks to the work at GNU!) and a powerful, reliable operating system kernel.

## **So far so good...**

In this article, we were presented with the first installment of the Field Guide for Investigating Computer Crime. We eased into the topic at hand by considering the basic questions about computer crime: what is it? how is it investigated? and, what skills and tools are needed by the computer fraud and abuse investigator? Along these lines, we discussed computer forensics, and some of its main endeavors and goals. We also outlined some specific hardware, and software tools required for computer fraud and abuse investigations, including an evidence preservation lab and case management system.

The next installment will present an overview of the computer forensics methodology that we've only touched on so far. We'll look at why a formal method for investigating computer crime is needed, what that method consists of at a high level, and whether or not all computer crimes need to be investigated with the method. Then, in additional articles, all of the gory details of how this methodology is carried out will be presented and discussed.

To read **The Field Guide for Investigating Computer Crime: Overview of a Methodology for the Application of Computer Forensics Part 2**, 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

[CCIPS](#)

*Department of Justice*

[Zeno's Forensics Page](#)

*Zeno*

[Reddy's Forensics Homepage](#)

*Reddy*

[Privacy Statement](#)

Copyright 2006, SecurityFocus