INFOCUS

Forensics on the Windows Platform, Part One

by Jamie Morris

last updated January 28, 2003

Introduction

Forensic examination of computer systems is commonly carried out by trained investigators using specialist hardware and software. The popularity of the Windows operating systems on both desktops and servers has made it a common source of evidence for such investigators. As a result, the range of tools available that can be used to analyze the Windows platform continues to grow. However, true forensic examination of a computer (i.e. where there may be a requirement to produce evidence in a court of law) does not take place only within the confines of a high-tech laboratory but also within the framework of current, relevant legislation and sometimes under the watchful eye of the media.

The experienced investigator knows that the success of a computer forensics investigation depends not only on the ability to uncover evidence from a computer system but also on the ability to follow proper methodology during the process of evidence collection and handling so that the evidence itself can be used in court. Such considerations may be of little interest to those whose goal is purely data recovery or intelligence gathering, but to forensic investigators engaged in the detection of crime or misconduct they remain of vital importance.

The first stage of any investigation is preparation that may begin even before a crime has been committed or a security incident detected. Importantly, it is not only investigators who are responsible for this preparation: it can also be carried out by the administrators of the systems in question. This article, the first in a two-part series about forensics on the Windows platform, will examine the preparatory steps that can be taken by both investigators and system administrators alike. While this series is concerned with Windows-specific investigations, this article will examine some basic, non-technical concepts that are applicable to all forensic investigations. The second article in this series will be much more specific to Microsoft Windows platforms.

Legal issues

The legal aspects of a computer forensics investigation center primarily on two main issues:

1. The requirements that need to be met in order for evidence to be successfully presented in court and, of course, considered legally admissible.
2. The need for the investigator to avoid the possibility of incurring legal action against himself/herself or the organization for whom he/she is conducting the investigation.

Frequently these two issues are linked, perhaps most obviously in the area of a suspect's right to privacy. A full discussion of current privacy legislation could form the basis of an entirely separate series of articles but, in short, anyone wishing to examine data associated with another person should ensure, before taking any action, that they are legally entitled to do so. This decision is usually arrived at by weighing the suspect's right to privacy against the rights and responsibilities of the investigating agency. Although simple in concept, this decision is not always clear cut in practice. Out-of-date legislation and new legislation without relevant jurisprudence can both combine to produce an element of uncertainty about what is or is not permissible in the eyes of the law. In high profile or high risk investigations specialist legal advice is strongly recommended.

Policies and Procedures

Often, an organization's privacy policy (if one exists) can prove crucial in weighing the rights of the suspect against those of the investigator. A well written privacy policy should make explicit how personal data is handled within an organization and under what circumstances this data may be laid open to scrutiny. Such a policy helps employees and employers to define a reasonable expectation of privacy. However, it is often not enough for an organization just to distribute a privacy policy, no matter how well written. To be most effective (not forgetting that a good privacy policy should benefit both the employee and the employer) the policy should be agreed to and signed off on by the employee.

Similarly, in the same way that a privacy policy can clarify how personal data is to be handled, a well written, distributed and agreed to "Code of Conduct" or "Acceptable Use Policy" can help define which user actions are acceptable and which are not. This can be important in investigations where suspects might otherwise be tempted to claim that they were unaware that their activities were unacceptable. The employee sign off form can provide proof of the employee's knowledge of and agreement to the policy.

Finally, an incident reporting policy and procedure are recommended to ensure that when incidents are detected they are reported to the correct department within an organization or to an external agency if appropriate.

Proper implementation of the above policies and procedures calls for them to be comprehensive, distributed to all relevant personnel, accepted by all relevant personnel, and regularly reviewed. The time and effort required to carry this out is well spent, as it can have a significant impact on the number of actual incidents that might require investigation, the number that are reported and the avenues open to investigators when computer forensic analysis is required.

When it's gone, it's gone!

Although computer forensics can sometimes seem like a type of modern day black magic, able to resurrect data once thought dead and buried, in reality forensic examiners can only retrieve data which is still physically present on a system (even though it may no longer be accessible through conventional means). Data that was never written to disk or has been completely overwritten is unlikely to feature in a subsequent investigation. Fortunately many operating systems offer the facility to record details of user or system activities through logging. Unfortunately for investigators many organizations fail to utilise the logging capabilities of their computer systems sufficiently for the data to be of use during an investigation.

The decision concerning which events and actions to log can be made by balancing the potential benefits of logging against the penalties incurred such as slower system response and increased disk space usage. The requirement for logging is likely to change as the perceived threat to a system or network changes, particularly since the option to log all events is rarely practical. A possible solution is to develop a simple system of logging levels that can be implemented as necessary, ranging from a base level that keeps a track of basic network activities (user logons and logoffs, for example) to higher levels that record more details about user and system activities and can be restricted to certain parts of the network, if necessary. It is also worth noting that logging is available on more computing devices connected to the network than just desktops and servers: routers, switches, firewalls, and even fax machines often provide logging capabilities.

These different logging levels are most usefully written down in another policy and procedures document that can be distributed to all network administrators. Clearly logging is useful during a forensic investigation as it records details of past activities, but it can also be useful in the detection of incidents that might require further investigation. Many logging systems offer the facility to generate alerts when certain events occur but at other times it will be necessary to review log files after they have been created. This can be done manually (although it may be very time consuming) or automatically using log analysis software. If the analysis software available is not suitable for the specific job at hand, then the use of Perl scripts is recommended as an alternative solution for log file analysis if the logs are available as, or can be converted to, text. Other issues to consider concerning logging are time synchronization between devices, how long logs are kept, where they are kept, and who has permission to access them.

Investigators in the corporate sector are often called in after an employee has left an organization to determine the employee's past activities. Logging can be very useful in this situation, as can the computing devices (such as laptops, desktops, PDAs, etc.) that the employee has used. Most organizations do not possess a huge surplus of such devices and they are often prepared for use by another user soon after becoming available. This preparation, usually performed by reinstalling a standard image to the device, can destroy potential evidence, so some organizations now make a forensically sound copy of ex-employees' computing devices soon after they leave. These copies can be stored for a certain period of time should an investigation prove necessary. This can certainly prove useful to investigators but organizations implementing this procedure should ensure that they have fully explored the legal aspects regarding employees' rights to privacy.

Building Your Forensics Toolkit

Forensic tools come in many different shapes and sizes from large, expensive, multi-featured commercial packages to free single-task utilities. The key to successful use of forensic software is, where possible, identifying which are the most appropriate tools for your environment and gaining familiarity with them before the need for an investigation arises.

Professional investigators will often use forensic hardware and software costing many thousands of dollars, but there are less expensive solutions. One of the most interesting is TASK (The @stake Sleuth Kit), which can be used together with the Autopsy Forensic Browser. TASK gives investigators the ability to examine images created with the "dd" utility for information of specific interest during forensic investigations (such as deleted files) and Autopsy provides an HTML-based interface through which TASK can be used and the results viewed. TASK and Autopsy work on various Linux and UNIX systems as well as Mac OS X but can also be used to examine Windows file systems.

Many of the free single-task utilities referred to above can also be of great help during the examination of a Windows-based computer. We'll look at some of these utilities in the next installment in this series.

Know What and What Not to Do

Ideally a computer forensic investigation will be carried out by trained, experienced personnel. However, this is not always possible and system administrators with little or no forensics experience may be called upon to carry out the initial stages of an investigation, often to determine if a more detailed and extensive investigation is justified. In this case, it is essential that the inexperienced investigator appreciates that the first steps in an investigation are often the most crucial and can determine whether or not evidence that is uncovered is admissible in court.

We will cover the steps necessary to uncover evidence on Windows platforms in the next article, but the most important thing to be borne in mind by anyone starting a computer forensic investigation is probably this: Whatever you do, don't alter the original evidence!

Many investigations are compromised by individuals using the suspect system itself to carry out a search for evidence. A good example of this is an investigator using the built-in Windows facilities of the machine under investigation to search for and open files. These actions have the potential to destroy data that is of evidentiary value as well as preventing any evidence uncovered from being presented in court. Whenever practical, a suspect machine should be shut down and imaged (i.e., a forensically-sound copy made); after which, only the image should be the subject of further investigation, thus ensuring the integrity of the original drive. More of this in the next article of this series.

Summary

The forensic analysis of computer systems is a fascinating and rewarding field but it exists within a wider social and legal framework that can have a direct impact on the way an investigation needs to be carried out. Furthermore, preparation can significantly affect the chances for success of a subsequent investigation.

In the next article of this series we'll get started with the fun stuff and look at how we image a Windows computer and where we can look for evidence of a user's activities.

Jamie Morris is the owner of Forensic Focus, a computer forensics news and discussion Web site.