

# Maintaining System Integrity During Forensics

*Jamie Morris* 2003-08-01

Deciding how to maintain the integrity of a system for use in a forensic examination can be a little like deciding which club to use to get out of the rough on the last hole of a golf tournament, i.e. the stakes are high and you never know if you've made the right choice until it's too late to change your mind (note: this analogy only works if you play golf as badly as I do. If you're a good golfer, or if you don't play golf at all, you'll have to come up with one of your own). While the use of good judgement may be more art than science, if we keep in mind certain basic principles and remember to think before we act we should give ourselves the best possible chance of a successful forensic outcome. These basic principles are the bedrock upon which any notions of a "best practice" must be constructed and will be the basis of this article.

It should be noted that this article is not intended to provide a list of steps for investigators to take, although I will include a list at the end to summarize the main points, but rather it is an examination of the issues which investigators concerned about "best practices" might care to bear in mind. There are two reasons for this. First, although computer forensic cases may share many common aspects it is rare that they are exactly the same. As a result, a single, specific step-by-step approach applicable to every situation is practically impossible to put together and is likely to be less than useful in the real world. Second, exactly what constitutes a best practice remains a source of some debate within the computer forensics world. What may be a best practice in Paris, Texas might be unacceptable in Paris, France (or vice versa!).

## **What is system integrity?**

Before we go on to discuss best practices in maintaining system integrity, a few words about what system integrity means in the context of computer forensics. Why, and to whom, is it important? Without getting too bogged down in the semantics of what "computer forensics" itself means, let's agree that it is the job of the computer forensics investigator to examine a computer system in the search for evidence which may be presented in a court of law. A fuller definition might involve other aspects of the investigator's responsibilities but we won't concern ourselves with them in this article. In other words, according to the definition the task before the computer forensics specialist is very much like that presented to detectives at a crime scene. As everyone who has ever read a detective novel knows, one of the first things the police do at any crime scene is to try to maintain its integrity. In this real-world scenario, maintaining the integrity of the crime scene means protecting any potential evidence from

being damaged or destroyed and preventing and false evidence from being introduced to the area in question. Maintaining the integrity of a computer system for use in a forensic examination is a similar process in principle but, as we shall see, presents very different challenges to the investigator.

Another equally important aspect of system integrity is the need for it to be achieved through compliance with current, relevant legislation. A sound understanding of the law as far as it relates to the discovery of electronic evidence should be the foundation upon which any subsequent investigation is built. After all if we go beyond the bounds of what is legally acceptable during an investigation any evidence which is uncovered is unlikely to be admissible in court. This is a point which can't be stressed enough, no matter how adept we are at uncovering evidence during a forensic investigation our goal remains to have this evidence to be presented in court. Sadly, complying with legislation is not always easy. Some laws are new and untested, others poorly constructed and in some places no immediately obvious legislation exists. All these things can combine to make the investigator's job even more difficult. Nevertheless, compliance with the relevant legislation should never be ignored.

In considering the integrity of electronic evidence in particular, we can see that such evidence needs to be protected from a number of undesirable outcomes -- namely, alteration (including modification or addition) or destruction, both of which could take place either accidentally or on purpose. Such changes or loss of data might occur for many different reasons, but typical situations might be where a suspect system is booted and/or examined while it is running or where a potential source of evidence is physically damaged, for example by dropping a hard disk or exposing it to unsuitable environmental conditions. We need to guard against these events and others when trying to maintain system integrity since a source of evidence which has been altered, or where a reasonable suspicion exists that alteration has taken place, is worthless in a court of law.

## **An example**

To examine the issues involved in greater detail let's take a typical situation where we need to maintain the integrity of a computer system for forensic examination. In this example we're going to imagine that an infamous drug dealer, Mr X, has been tracked down to a supposedly secret location and we've been assigned to the task force charged with arresting this top criminal. Our specific responsibility is to seize his computer so that it can be searched for potential evidence of his nefarious activities. On the face of it, it's a simple enough task: we

enter the premises, locate the computer, transfer it to the evidence vehicle outside and then transport it back to the station (or office, if you're a civilian investigator). At all times the computer is under our control and we can vouch that nobody else had an opportunity to touch it. If there's evidence to be found, we'll find it during a later examination. Case closed. Or is it?

When we located the computer did we check if it was powered on? Did we need to check for potential active network connections? Running processes? Perhaps the greatest difference between a "real world" crime scene and that offered by a computer is that whereas the former can often be isolated from change by surrounding it with protective material and posting a guard (let's ignore the effects of decomposition for now) the latter offers no such simple solution unless the device happens to be powered off at the time of discovery. A running computer poses a number of issues to the investigator charged with its seizure and forensic examination. Primarily, should the device be powered down before analysis, and if so, how?

### **To power off or not**

The first step to take when approaching an active, powered on and running computer is simply this: STOP and THINK. The necessity for considered action arises from the fact that there is no standard step-by-step procedure for maintaining the integrity of a computing device which will be applicable in every situation. Every situation requires careful consideration of the nature of the case and the computing device in question. What may be a sensible set of actions for maintaining the integrity of one machine may in fact lead to loss of evidence on another.

Let's look at the main issues involved here. First, based on the nature of the investigation, where is crucial evidence likely to be located on the computer? Which component or components of the system are we really interested in maintaining the integrity of? Is key evidence likely to be on the hard drive or in memory? The majority of computer forensic investigations involve the analysis of hard drives which are no longer attached, physically or logically, to a running operating system on a suspect's machine (often the drives themselves will contain the operating system in question). This makes sense as the vast majority of information contained within a computer system will usually be found on the hard drive, rather than in memory. However, the contents of RAM in an active computer system undoubtedly hold some information and occasionally this can be vitally important to a case. For example, data which is likely to be found encrypted on a disk might be found in an unencrypted state in memory, or a running process might need to be identified and examined before power is removed. Any such information in memory will be lost when the power supply to the device is

removed, so we need a strategy to guard against this if we decide that the evidence we are looking for is most likely held in memory.

One technique might be simply to power down the computer using the standard OS-based shutdown routine in the hope that the data in question will be written to disk. This can be an effective technique if we have reason to believe that the data will indeed be committed to disk, but it is not without risk or controversy. First, we are changing the state of the evidence (i.e. the hard drive data) through our own actions, which is a violation of one of the fundamental principles of computer forensic examination. Second, we run the risk of a routine being triggered during the shutdown procedure (either as part of the normal shutdown process or as part of an attempt by the suspect to cover their tracks) which destroys vital data. Another method is to carry out a live examination and attempt to analyse the state of system memory while the suspect device is still running. This is usually considered somewhat more controversial from a forensic standpoint. As before we are likely to alter the state of the system through our own actions. Furthermore we need to be as sure as possible that the computer has not been configured to return false information and that the results returned can be relied upon. In this case we might consider the use of our own statically linked, trusted binaries. Nevertheless there may be situations where a live response is called for, not only for evidence retrieval from memory but also in cases where it is undesirable to shut down a system for analysis. Finally, when considering the possibility that evidence is likely to be held in memory, we should not forget that the very data we are searching for may have been swapped out to the hard disk and no longer be present in memory anyway (although some software may guard against this by preventing the relevant areas of memory being paged to disk).

As we can see from the above, retrieving information from memory for use as evidence while trying to maintain a level of integrity that allows the information to be used in court is not a trivial task, although there may be occasions where it is either desirable or necessary to attempt to do so. In most cases though, the investigator will be content with securing the contents of the hard disk, although the question of how to deal with an active machine still remains. In many cases it makes sense to simply turn off the power on a running computer and remove the machine to a forensic lab for examination. Reasons for doing so could range from the desire to remove the machine from a potentially hostile environment in which it might be damaged, to the need to use specialist equipment not available "on scene". It may be equally necessary to examine the machine where it is found, especially if time or discretion are important factors in the case.

## **Pulling the plug, or...**

Once the decision has been made to remove power from a running system the next question is simply, how? Again we face a choice: removing all power immediately ("pulling the plug") or attempting to perform a graceful shutdown. There are various arguments for and against both courses of action and the ensuing debate is one of the longest running in computer forensics. As we have observed above, pulling the plug will most likely leave you with the current contents of the disk intact but leave you without whatever information was held in memory (it may be important to note that "pulling the plug" should be taken quite literally and does not refer to using a system's power or on/off switch which may initiate a controlled shutdown. Also, if power is supplied through a UPS, we should make sure that the power FROM this source is removed, not the power TO it). It has also been argued that pulling the plug, and thus preventing the system from shutting down as intended, may render it incapable of booting again (not necessarily a problem but it might be important under certain circumstances). In comparison, shutting the machine down gracefully may avoid some of these issues but the threat of data destruction or alteration during the shutdown process, and the consequences of such an event in a forensic investigation, cannot be overstated. In my own experience, "pulling the plug" has often been the most appropriate response to securing a system for forensic examination but each situation must be considered individually.

Once we have addressed the issue of preserving system integrity before and during seizure, we now need to consider how we maintain and demonstrate the integrity of the data which has been secured. Specifically, how do we show that the evidence which we present in court is indeed based on the data which was captured at the time of seizure? The most common technique used to demonstrate that data has not been altered is that of "hashing". Hashing involves the use of a mathematical algorithm to create a very large number based on the contents of a data source (e.g. file, directory, partition, hard disk, etc.) The value of creating such a number, or hash, then derives from the fact that changing just the smallest element of the data source will result in a completely different hash being generated by the same algorithm, thus showing that the original data has been altered in some way. It is good forensic practice therefore to create a "hash" of the data which has been secured as early as possible during an investigation so that evidence presented at a later stage can be recognized as being derived from the data which was seized.

There is a very interesting debate at the moment concerning exactly how and when this hashing process should be performed, in particular whether it is acceptable to perform the

initial hashing during the imaging process or whether an evidentiary source needs to be hashed prior to imaging. I recommend that anyone wishing to keep up to date with this issue join one or more of the computer forensic mailing lists available on the Internet.

## **Imaging and analysis**

Having seized the data and taken steps to create a hash of the original data, the next step in an investigation is usually analysis. In other words, now that we've got our hands on what may be the source of potential evidence, it's time to start looking for the evidence itself. There are many tools and techniques available to assist with computer forensic investigations and the correct selection of the right ones will depend on a variety of factors. Regardless of which means we use the overriding principle which should govern our investigation is that the analysis should take place on a forensically sound copy, or image, of the seized data, rather than the original data itself. By confining our analysis to such a copy we avoid any risk of altering or destroying evidence on the original, a cardinal sin in forensic examination. However, a common "gotcha" here is the risk that a potential source of evidence, such as a hard drive, is altered during the imaging process perhaps by being booted up or by data inadvertently being written to it. Extreme care should be taken during this stage of an investigation to minimize the risk of such an event. There are a number of software and hardware solutions on the market (usually termed "write blockers"), the use of which is recommended.

The next priority in creating a forensically sound copy (after ensuring that the procedure will not alter the original data source) is to ensure that the imaging process retrieves ALL data from the source device. A normal copying function will only transfer information found in files and directories but in a forensic examination we will almost certainly also be interested in the areas of disk which may once have been allocated to such data structures but are no longer part of the current filesystem (by having been deleted, for example). Such areas may be those which have been marked by the operating system as available for future allocation or even parts of the disk which have been allocated for current data storage but are not completely full with data (the empty areas being termed "slack space"). In any event, our aim is to copy every single bit of data from the original data source and thus create a platform for analysis which can be said to be "forensically sound". Again, there are a variety of tools available to the investigator to help achieve this goal. Through the use of these tools we aim to ensure that the care we have taken both in maintaining the integrity of the system under investigation and in performing the imaging process results in an accurate copy of the system at the time of seizure.

After a copy has been made successfully, we need to make sure that the original data remains intact and is not damaged or altered through mishandling or storage in inappropriate conditions. This is commonly achieved through using an established evidence handling procedure which might involve tamper proof evidence bags, a secure climate-controlled storage area, evidence book, and so on.

During all of the above steps, we as investigators will have had to make decisions based on various factors and choose between various courses of action. If we are called to court to present our findings we are likely to be questioned about why we made the choices we did. If so, an invaluable aid to memory are detailed notes taken during the investigation. These notes should cover everything from a description of the physical location of the computer, through to a detailed description of its component pieces up to and including a description of the handling and storage methods used. Reference to these notes at a later stage can help to show that the integrity of the system in question has been maintained through adherence to proper procedures.

## **A brief review**

To sum up, let's take a look at some of the issues which we might want to think about when discussing best practices in maintaining system integrity for forensic examination:

1. Stay current on relevant legislation. The goal of any forensic investigation is not only the discovery of evidence but the ability to present that evidence in court. To do this we need to ensure that all aspects of an investigation are strictly legal and that the integrity of the data presented cannot be called into question.
2. Decide where on a computing system any crucial evidence is likely to be located, and direct the investigation towards its seizure and analysis, where possible, without violating the basic principle of not altering the data source.
3. There is a need to show that any evidence presented derives from data on the source device which was present at the time of seizure, and that no data on the source device has been altered thereafter.
4. Perform analysis on a copy of the original data, not on the original data itself. Take care to ensure that the original data source is not altered during the copying process.
5. Ensure proper handling and storage procedures for seized items.
6. Document your actions. In order to show that an investigation has taken place in

accordance with the relevant legislation, the creation of detailed notes can be invaluable.

The best way to draw all these points together in a useful fashion is to create a policy and/or procedure before an investigation takes place so that important issues can be discussed and agreed upon beforehand. The short list above is by no means exhaustive and should be expanded upon to take into account the responsibilities and requirements of each individual investigating agency.

## Summary

At the start of this article I alluded to the difficulty of defining exactly what constitutes best practice in this area of computer forensics. I would offer two possible definitions. One is to say that best practice involves following accepted, published guidelines (where they exist) and ensuring that your actions as an investigator comply with all relevant legislation. This is undoubtedly a useful definition and should be a baseline for all forensic examiners. Another is to see best practice as the actions required to carry out an investigation properly, thoroughly and impartially in accordance with (and sometimes in the absence of) current legislation. Whichever definition we choose, as long as we continue to discuss these matters and legislation is informed by the results of such debate, then our notions of what constitutes best practice stand a good chance of influencing common practice wherever we are.

---

*Jamie Morris is the owner of [Forensic Focus](#), a computer forensics news and discussion website.*

### Author Credit

View [more articles by Jamie Morris](#) on SecurityFocus.

[Privacy Statement](#)

Copyright 2006, SecurityFocus