

Preserving Digital Evidence

Upon arriving to work one morning you check your voice messages. There is a message from the President of the Company. He wants you in his office as soon as you get in and he sounds very serious. You search your mind to see if you have done anything that might warrant a firing. You quickly conclude that you haven't and scurry to his office. There he confides in you that he suspects that his CFO is stealing from the company, and he wants you to gather evidence from his email, internet and hard drive for the possible court case against the CFO. If you can gather sufficient evidence, the CFO will be terminated with cause and an action will be brought against him to recover the lost funds.

The President confides in you that he suspects that the CFO has set up a dummy company owned by him and has been authorizing payments to that dummy company for some time now, but he has no hard evidence to prove it. Before leaving his office he tells you that he has sent the CFO away on a two day business trip so you will have unfettered access to any of his electronic information. As you are about to leave the President's office, he stops you, looks you in the eye and lets you know in no uncertain terms that if you mess this up or if you tell a single soul on this planet, you will be fired.

There are a few key messages that we need to understand from what the President has told us. First, if the allegations are true, this matter will end up in the courts. There may be a wrongful dismissal suit and secondly, there will be an attempt in the courts to recover the lost funds. So whatever you do, you must preserve the evidence in a way that will be acceptable to the courts. The other thing to note is that the CFO is no dummy. He will likely not have left "evidence" laying around on his hard drive and would have taken reasonable measures to hide it. Now my advice to anyone who is in this situation is that you should seek the help of professionals who are trained in the preservation and examination of digital evidence. However, when you suggest this to the President, he insists that he wants no one else involved and you and you alone are to conduct the investigation.

The remainder of this article will focus on how to proceed with the investigation given the circumstances your President has left you in. This article is by no means a complete step by step guide to digital evidence preservation. However, it should give you a sense of how to proceed and what to watch out for. Everything you do from this point on should be viewed in the context that you are in a court room and the defense attorney is accusing you of altering the evidence. You must be able to prove to a nasty attorney (sorry to all my legal friends) that at no time did you alter any of the evidence.

So, where should you start? First, get a clean empty note pad and start writing. Write down the date, time and summary of your conversation with the President. Write down everything he told you. Then go to the CFO's office and before you touch anything start writing some more. What do you see? Is the computer on or off? Are there diskettes, CD's, DVD's, USB drives or Zip drives laying about? Are there any unusual connections on the back of the p/c that you don't recognize? Is there a key catcher there? Did you record the time of when you entered the CFO's office? Now get a digital camera and take pictures before disturbing anything. You will want to have a picture of how the office looked before you touched anything, a picture of the computer (whether it was on or off) and a picture of the rear of the computer. Most importantly, since we are going to be moving a few things around and we know the CFO will be back in two days, we will want to be able to put the office back together without arousing suspicion.

If the computer was on, power it off by pulling the power cord from the base of the unit. Most computers today will go into an automatic shut down mode if you hold onto the power button. When you go into a shutdown mode, you are updating the date/time stamps of certain files on the computer and that nasty defense attorney will suggest that you altered the contents of the files on the CFO's hard drive. Given that the CFO was away on business and certain files were altered; he will immediately put you on the defensive and bring into question the integrity of the evidence.

Now that there is no power to the computer, open up the case to see what is inside. Is there a second hard drive that is not hooked up? Is there anything unusual inside like a hidden USB drive? First we need to disconnect the hard drive. Assuming this was the only hard drive, now we want to boot up the machine (with no boot device present) and go into the CMOS. Bring up the date and time screen. Take a picture of that screen and compare it against a known correct time. For example, you could use www.worldtimeserver.com (on the wireless laptop you brought with you) and compare that time against the CMOS time of the CFO's machine. For obvious reasons, it is very important to establish the relative time difference between the two.

Next we need to get at the data on the hard drive without altering any of its contents. If we were to attempt to "boot up" the hard drive we would have altered hundreds of files during the boot up process. So what we do is use a write blocker and attach the hard drive to the write blocker. We then take a bit stream image of the hard drive. Encase, sold by Guidance Software, is one of many tools available that will take a bit stream image of a hard drive through a write blocker and allow you to interrogate the hard drive. Some of the many features of Encase will allow you to view any email that is stored on the hard drive, view internet usage, look at deleted files, and compare the file extension of a file against what the file actually is. A simple hiding technique is to rename a document file (.doc) to a picture file (.jpg). Encase will also do searches on the entire hard drive including unallocated clusters. In future articles I will deal more with the specifics of what to look out for on a hard drive using various tools.

Your Company is a medium size company and email is stored on an "Exchange" server and the client on the desktop does not store the mail files locally. How then do you capture this information in a forensically sound manner? First, you need to find last night's backup tapes for the exchange server and label them appropriately. You should also take a second backup copy. Restore from the second backup copy to a hard drive that you can then analyze using your email client. The same applies if you are using a proxy server for your internet traffic. Take a second backup copy of the proxy logs and mark them appropriately. Restore from the second backup copy to a hard drive so that you can have a look at these logs as well. If those nasty defense attorneys challenge you on altering the evidence that was presented, you can provide them with two sets of backup tapes that contain the same information.

Finally, you need to find a place to store your note pad with your copious notes, your bit stream image of your hard drive and the backup tapes. You also need to ensure that only you had access to this place and no-one else. You must preserve the "Chain of Custody" on the evidence to ensure that the evidence could not be tampered with.

To conclude the story, since we all like happy endings, you found the evidence on the hard drive that supported the President's allegations, the CFO was dismissed and paid back all of the money that he stole, and you got a hefty raise.