

Article

ASK OUR EXPERT:

What Can Computer Forensics Do For You?

The following are frequently asked questions pertaining to computer forensics and answers from our resident expert, Lee Neubecker.

What do you recommend as a best practice for preserving electronic data on a computer?

One of the most important things that companies need to do is to make sure that they do not spoil the evidence by looking to see what the employee was doing. In many cases, right after someone departs, the manager or someone from IT will look through the computer to see what files were recently accessed. The problem with that is the employee may have downloaded files to CDs to take with them. If someone surfs through a computer to see what was stolen, they are altering the file metadata, such as the date the file was last accessed. It may cause a file that was burned to CD along with other collection of files to have its last access date altered. In computer forensics, we often look for clustering of files with similar dates and times. For instance, if someone burns a number of files to CD, the last accessed time may be a second apart on files that were recently burned to CD. Frequently, we can figure out what was burned to CD by looking at the access dates because when the computer reads the file to write it to CD, it alters access dates. The manager who accesses the computer to look around has just caused the access dates to be modified, so it makes it more difficult for forensic experts to piece evidentiary information together.

The most important step is first to make sure the evidence does not get altered, and in most situations (e.g. Windows operating systems), simply pulling the plug from the computer works. Pulling the plug prevents evidence spoliation and preserves relevant last accessed dates. Exceptions to that are Linux, servers and other more complex file structures that do not recover well from a power loss.

If someone needs to reuse the computer, they should remove the hard drive in question and buy a new hard drive for the computer. That way the evidence is reasonably preserved. They can keep the evidence hard drive in an envelope sealed by a signature and clear tape, and that way any evidence alteration can be detected by tampering of the package.

What is the most effective method of authenticating evidence?

The first step in authenticating evidence is that you need to preserve the original evidence by removing it from normal use and sealing it from possible tampering. Once you preserve the evidence, it needs to be forensically copied in a way that does not alter the original. The copy is then used by experts to perform their analysis. Before performing the analysis, the evidence needs to be authenticated. To authenticate the evidence, in essence, is to certify that the copy is exactly the same as the original.

In our profession, a hash value is used to authenticate evidence. A hash value is generated when you apply a hash algorithm against a collection of 0's and 1's that exist as data on a hard drive or any other type of storage media. That value is such that altering a single character in a Word document, for example, changing an upper case S to a lower case s, would cause the collection of 0's and 1's on the storage media to be altered. This would then cause the hash value generated to be something totally different. Therefore, when we copy data, we are copying all the 0's and 1's on the most micro level of the storage media. We are applying the hash algorithm, and as an end result, we are getting a unique hash value, which is much like a digital fingerprint. After copying, we apply that same algorithm to the copy, for the same number of sectors. If the hash values match, we know we have a perfect copy. Once we have copied the evidence and authenticated it, then we are ready to work with the data.

If the judge allows electronic discovery without limitations, is it advisable to ask for a printout of all files on the computer?

Before doing a print production, it makes a lot of sense to apply technology to eliminate a lot of the unnecessary information. Unique to computer forensics is the ability first to tell what is on the hard drive—files that exist on the hard drive, deleted or not, when they were accessed and created, how large they are, etc. That is a great starting point because it allows you to assess, if you were to print the files, how many pages would result and what the universe of data is.

Once we know what is on the hard drive, we can perform a hash analysis whereby we analyze every individual file's hash value and compare the fingerprint of the individual file against the NIST (National Institute of Science and Technology) database, which publishes a database with the hash values or fingerprints of all known files that exist. The NIST hash database contains files that appear on operating system CDs and software applications. After analyzing and comparing all the files on the subject hard drive against this database, we can eliminate gigabytes of information that are in no way pertinent to that user's created data. We can remove those files from the list,

which eliminates useless help text files and other files that come with your computer. That saves the client a lot of time, as well as money.

In addition, if our client provides us with the universe of intellectual property data (e.g. CAD drawings, price books and customer directories) on a CD, we can generate the hash values for each of the individual files. These values are then used to compare with that of all the files that exist on the subject hard drive we imaged. If there is a match, it is evident that our client's intellectual property exists on the subject computer. At that point, we can begin to explore how it got there, when it got there, what other places the file was stored and other critical information.

What is Metadata?

Data about data. Metadata can provide information about a specific file or document. For example, filename, size, when created, last modified, last accessed and total document editing time are all considered valuable metadata. Sometimes individuals make an effort to alter metadata. When a person tries to cover their tracks by tampering with metadata, inconsistencies across various metadata points can sometimes reveal clues of evidence tampering. Only an expert skilled in forensic examinations has the necessary skills and experience to testify credibly in a court of law relating to computer evidence tampering.

What is Storage Media?

Storage media are devices that store application and user information. The primary storage media for a computer is usually the internal hard drive. Most internal drives are regular IDE hard drives that come with the computer. A removable drive is another popular storage device that is usually connected by firewire, USB, or parallel port (e.g. portable Zip drives, Jaz drives, or CD/DVD drives). Newer forms of external storage include USB thumb drives and camera storage media.

Most external drives enable flexible data transfer from one computer to another. A computer that has had external drives connected to it usually has evidence in the computer's registry of using the subject device. When performing a forensic examination during discovery proceedings for litigation, determining if external drives were connected to the computer may help in obtaining additional evidence for discovery.

What Is Forensic Hard Drive Imaging?

When a computer is identified as possibly containing electronic evidence, it is imperative to follow a strict set of procedures to ensure a proper (i.e. admissible) extraction of any evidence that may exist on the subject computer. The first thing to remember is the “golden rule of electronic evidence”—never, in any way, modify the original media if at all possible. Thus, before any data analysis occurs, it usually makes sense to create an exact, bit stream copy of the original storage media that exists on the subject computer. This may include a single or multiple hard drives, floppy disk(s), CD(s), Zip drive(s) or DVD(s), plus many other types of storage media that now exist. Imaging the subject media by making a bit-for-bit copy of all sectors on the media is a well-established process that is commonly performed on the hard drive level, hence often referred to as hard drive imaging.

The creation of a true forensic hard drive image is a highly detailed process. If you do not have it performed by a trained professional, you may severely compromise your chances of obtaining admissible evidence as a result of your discovery efforts. Also, to avoid accusations of evidence tampering or spoliation, it is a recommended best practice that imaging be performed by an objective third party. Suggested protocols for hard drive imaging can be found within guidelines standardized by institutions and organizations like the Department of Justice (DOJ) and the National Institute of Standards and Technology (NIST).

As you hire a computer forensics expert, know that he or she can choose among a large number of software and hardware to obtain a forensic image. What is important is that you qualify the expert’s experience and that you ensure a rigid process by asking the right questions. A good start is to always make sure that the integrity of all evidence is maintained, chain of custody is established, and all relevant hash values are documented.

Once imaging is completed, any good tool should generate a digital fingerprint of the acquired media, otherwise known as a hash. A hash generation process involves examining all of the 0’s and 1’s that exist across the sectors examined. Altering a single 0 to a 1 will cause the resulting hash value to be different. Both the original and copy of the evidence are analyzed to generate a source and target hash. Assuming they both match, we can be confident of the authenticity of the copied hard drive or other media.

The industry standard for imaging currently recommends the use of the MD5 algorithm. The creator of the MD5, Ronald L. Rivest of MIT, describes the algorithm as follows:

[The MD5 algorithm] takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input... The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.

Mathematical jargon aside, the above statement simply says that the MD5 is an excellent method of verifying the integrity of data. An MD5 value obtained from the image of the hard drive should match the value of the original hard drive. Even the smallest modification on a hard drive, for example, adding a comma to a MS Word document, would vastly change the resulting MD5 hash value.

While it may seem plausible to utilize internal IT personnel to render an image of a suspect hard drive, keep in mind the possible consequences. Hiring third-party computer forensics experts will ensure safe handling of evidence. A qualified expert will follow industry standards to avoid spoliation and will help to refute the charge of sabotage by an internal staff member who may know the key individual(s) connected to the case. A third-party expert will also establish a chain of custody that guarantees another layer of protection to the evidence.