An Introduction to Computer Forensics

Jim Ed Crouch, NSCI
December 16, 2010

Computer forensics is one of the four sub-disciplines – along with network, database, and mobile device forensics – that fall under the branch of forensic science known as "digital forensics." As the name implies, Computer Forensics uses analysis techniques to gather evidence from desktops, laptops, servers, and peripheral devices for the purpose of investigating suspected illegal or unauthorized activities. The goal is to perform a structured investigation while maintaining a documented chain of evidence that can withstand the legal scrutiny of a court of law, for either a criminal or civil proceeding.

Very few users of a computer are aware of the vast amounts and types of information generated and stored by the operating system and software applications resident on the computer. In addition to the active data easily seen by users, there is the so-called metadata – data about data – that is not displayed onscreen. An example of this is the date/time stamp showing exactly when certain data are created. Other examples include log and hidden system files and information recorded in a non-text format. Also available on a hard drive and other media are "latent" data – files that have been deleted but reside in "unallocated clusters" or "slack spaces" and haven't yet been overwritten. Specialized tools and expertise are required to access these data and to understand their relationships and relevance within the scope of the investigation.

Computer forensics experts typically conduct their investigations and gather evidence not from the original device but on a perfectly-replicated digital image of the original. This is done to avoid the legal complications created by either an actual or perceived alteration of the central piece of evidence involved in the investigation. To preserve this evidence in its original state and avoid accusations of tampering, forensic examiners conduct a step-by-step, scientific investigation that includes precise documentation of each activity throughout the entire process. One of the early steps in the investigation is the imaging of the hard drive.

To ensure the created image is an exact replica of the original, investigators use so-called "hashing" tools to compare original hard disks to copies. These tools analyze data and, based on that data, assign it a "hash" number. If the hash numbers on an original and a copy match, the copy is a perfect replica of the original. The best explanation of hashing we've seen is contained in a 2008 paper, "*What Judges Should Know About Computer Forensics*," written by Craig Ball, a trial lawyer and certified computer forensic examiner:

> *"The creation of a forensically competent copy entails a second step. It is not enough to simply make a faithful copy of the disk drive; a forensic examiner must be equipped to irrefutably demonstrate that the copy does not deviate from the original, both immediately after it is created and following analysis. This is typically accomplished using some mathematical sleight-of-hand called "hashing." Hashing a disc creates a digital fingerprint; that is, a small piece of data that can be used to positively identify a much larger object. Hashing is a form of cryptography that relies upon a concept called "computational infeasibility" to fashion unique digital signatures. Essentially, the entire contents of any stream of digital information is processed by a specialized mathematical equation called an "algorithm" that works in only one direction because it would be a gargantuan (i.e., "computationally infeasible") task--demanding hundreds of computers and thousands of years--to reverse engineer the computation. The bottom*

> *line is that if the bit stream copy of the data is truly identical to the original, they will have the same hash values; but, if they differ by so much as a comma (well, a byte), the hash values will differ markedly. The computational infeasibility means that someone trying to pass a doctored drive off as a bit stream copy can't make changes that will generate an identical hash value. There are a number of hash algorithms floating around, but the two most frequently employed in File recovery programs search for and restore deleted data. These programs locate data that the computer has marked for deletion but has not yet been overwritten, sometimes resulting in an incomplete file."*[1]

The sequence of events employed by the forensics examiner involves the use of several different tools to image, analyze, and document the evidence. Disk imaging software and write tools copy the information from the hard drive and other storage media such as those connected through USB ports, reconstructing it bit by bit while preserving the exact organization of all files. After making the copy, investigators lock the hard drive in a secure facility and conduct the investigation exclusively from the digital copy. Because of the staggering capacity of modern computers, it's very difficult and time consuming to search computer files manually. Investigators thus use analysis software with specific capabilities to sift through all the gigabytes of data, looking for specific content. One example of this would be an investigation that includes a suspect's internet activities, whereby the examiner uses a program designed to search and evaluate browser cookies. To access protected data, analysts use software with decoding and password-cracking capabilities.

So what should managers and supervisors know about computer forensics and how should they respond when there is reason to suspect that some incriminating evidence might exist on a computer? The first question to ask is whether the situation warrants the use of a qualified computer forensics investigator. Commonly cited reasons to justify the employment of forensics are self-defense and management of risks. Companies must have a way to detect and prevent future incidents and maintain legal recourse when required. It is also important that any response to malicious actions include a process that preserves evidence in accordance with The Federal Rules of Evidence, thus preserving an organization's options. Knowledge that an organization is willing to employ a forensics examiner can also have a deterrent effect. Gathering computer forensics evidence is, of course, also helpful in confirming or dismissing suspicions that illegal or unauthorized activities have occurred.

Computer forensics should be employed when there is a serious risk of a lawsuit, compromised intellectual property, loss of competitive capability, or damage to the organization's reputation. However, like many other activities, the use of forensics often boils down to a cost/benefit analysis, but this is often a judgment call made by company. If the organization's leadership believes there is a reasonable likelihood that the situation could escalate into a court trial, then it is advisable to hire a qualified computer forensics examiner. Costs of doing so can run into the thousands of dollars, but may very well be worth it. In recent years, companies have used the threatened or actual use of computer forensics – regular, random examinations of workstation hard drives – to discourage their employees from conducting unauthorized activities. However,

[1] http://www.craigball.com/What_Judges_Computer_Forensics-200807.pdf

the cost/benefit analysis of this deterrence activity is as problematic as the Obama administration's promise of "saving" jobs via the stimulus. How do you quantify or otherwise measure such non-events?

Computer forensics may not be required when computers have played only a minor role in the activity being investigated. However, as noted in a 2001 report by Veritect, this basic question of the exact extent to which a computer was involved may also require forensics (i.e., we may need to examine it to decide whether there's a need to examine it).[2]

After we've made the decision to call in a forensics expert, we should understand that his investigation is conducted in a way that ensures finding, preserving, and preparing evidence. In another of Ball's outstanding articles, "*Computer Forensics for Lawyers Who Can't Set a Digital Clock,*" there is this advice for lawyers – called the five A's – that can also apply to managers responsible for balancing the need to protect not only the company's bottom line, but also the rights of the suspect:

1. ***A****dmissibility must guide actions: document everything that is done;*
2. ***A****cquire the evidence without altering or damaging the original;*
3. ***A****uthenticate your copy to be certain it is identical to the source data;*
4. ***A****nalyze the data while retaining its integrity; and,*
5. ***A****nticipate the unexpected.*[3]

Ball goes on to say, " These cardinal rules are designed to facilitate a forensically sound examination of computer media and enable a forensic examiner to testify in court as to their handling of a particular piece of evidence. A forensically sound examination is conducted under controlled conditions, such that it is fully documented, replicable and verifiable. A forensically sound methodology changes no data on the original evidence, preserving it in pristine condition. The results must be replicable such that any qualified expert who completes an examination of the media employing the same tools and methods employed will secure the same results."[4]

How do we choose an examiner qualified to properly perform the "find, preserve, and prepare evidence" functions in accordance with The Federal Rules of Evidence? Veritect's list of qualifications from 2001 still stands:

- Prior experience in computer forensics examinations
- Specialized training in computer operating systems
- Specialized training in evidence handling and investigation techniques, including information recovery tools
- Documentation of processes used in forensics examinations

[2] "What Lawyers and Managers Should Know About Computer Forensics, Veritect, June 2001
[3] http://www.craigball.com/_OFFLINE/CF4_0807.pdf
[4] Ibid

- Personal integrity: Investigators must withstand scrutiny on both technical ability and personal integrity
- Investigative ability: Investigators need logical thinking, the ability to uncover and understand cause and effect, and possess an open mind
- Demonstrated knowledge of the Federal Rules of Evidence
- Experience testifying as an expert witness
- A laboratory stocked with tools for evidence recovery
- Quick reaction time to handle incidents before evidence is destroyed and to report evidence perpetrators disappear. This also is a compelling reason to keep an examiner on retainer[5]

Prior to the arrival of the examiner, managers should observe a simple rule to preserve the evidence and avoid having the case thrown out of court on day one of the trial. Simply stated, this advice is, don't disturb the scene of the crime, or better yet, "I no touchy nothing." If the computer is turned on, leave it on; if off, leave it off. Do not move the computer or any of its peripheral devices, and do not rearrange any of the objects surrounding the machine. Do not attempt to run any programs on the machine, and do not allow any of your system administrators to tamper with it any way.

Finally, after the arrival of the examiner, expect to see decisive initial actions to preserve evidence, combined with a very methodical approach to gathering it. Think of the famous slogan used by fighter pilots in aerial combat: "Let's slow down and kill him quicker." Further, do not be surprised when the examiner assumes the suspect is an expert, professional criminal and sophisticated technical expert at the outset; he should assume this until proven otherwise. The forensics investigator may decide to exercise extreme caution to preserve evidence and ensure the suspect cannot successfully employ countermeasures – such as software used to wipe data – against the forensic techniques being employed. If the examiner says to you, "Stand back 30 feet while I push this button," you'll know why.

[5] "What Lawyers and Managers Should Know About Computer Forensics, Veritect, June 2001