



COMPUTER FORENSICS DESERVE A PLACE IN YOUR HUMAN RESOURCE TOOL KIT

Executive Summary

Computers contain evidence useful in many human resource circumstances. Analyzing employee computer usage can sometimes quickly resolve allegations of discrimination, sexual harassment, and unfair discharge. Since computers are such a pervasive part of most employees' work lives, analysis of data stored on these computers helps address these issues. Internal investigations are incomplete without electronic evidence.

Computer forensics can also combat theft of trade secrets. No business wants to allow a competitor to hire an employee and steal valuable confidential information. In most cases, the stolen information is stored on computers, with computers used to initiate the theft.

Computer forensics can trace the steps used by an employee to provide you the evidence needed for fair and resolute decisions. Most operating systems store massive amounts of information. Much of this evidence is difficult to eliminate.

The cost of properly collecting and analyzing this evidence is miniscule compared to what your company is already paying for such incidents. When done properly, computer forensics generate significant savings. We can perform this work remotely for clients in any location.

Computers record massive amounts of information about user activities. Both applications and the operating system record this information, sometimes in more than one location. Deleting files, emptying the recycle bin, and clearing the memory of browsers or other applications does not remove information from all locations.

Because of this, important information can be obtained from rather obvious (if you know about them) usage logs and storage. A computer user that wishes to cover his tracks can clear some of this information, but some subjects are careless, unsophisticated, and/or surprised by your investigation. However, even crafty and sophisticated people will have trouble eliminating everything. Even the act of eliminating information will leave tracks.

When dealing with those crafty and determined people that think they can cover their tracks, the "magic" of computer forensics is well worth its cost. In most investigations, here is the type of information you will receive:

- Deleted files (or portions thereof) that remain on the disk because subsequent activity has not yet overwritten them.
- A listing of deleted file names, even if the files themselves cannot be recovered. This is useful in showing use of unauthorized programs, or files with suspicious names.
- Internet sites visited, regardless of the browser settings or deletion of the browser history. This information is stored in hidden system files, parts of the Windows registry, and as remnants of web addresses that remain in "unoccupied" file space.
- Information and graphics from internet sites visited (we often find images that are clearly against almost every company's policies).
- The existence of suspicious applications, or the fact that they were used. Examples of troubling applications are those used to transmit files, communicate with unauthorized remote computers, prevent data recovery, crack passwords, encrypt files, or perform computer hacking.



Our computer forensic work saves considerable money,

- Information remaining in swap files, page files and other temporary Windows files. These files generally show what the user was working on recently, even if not otherwise saved.
- Information contained in hidden and password protected files from just about any well-known file type.

Although perhaps obvious, an investigator can sort and search computerized text and numeric data using powerful software. This allows the investigator to find information rapidly, using key word searches. Similarly, the investigator can typically identify target file types, including files where the person being investigated attempts to hide something by changing a file extension.

Even though some data may be easy to retrieve (e.g., files that remain intact, data within recycle bins, browser history and temporary files), you still need to be able to prove that the

Most people have no idea about the wealth of information that remains on their hard disk.



subject is the one responsible for the evidence. Even for the evidence that is obvious, procedures that prove the source of the data are very important.

How Should One Deal with this Fragile Evidence?

Merely booting the subject computer in a Windows environment will alter critical date stamps, erase temporary data, and cause hundreds of writes to the drive. Each of these actions overwrites data that may be important to the investigation. Therefore, until you obtain expert assistance, if the computer is on, leave it on. If it is off, leave it off.

Specialized computer forensic software ensures that the subject's computer is not altered in any way during the evidence acquisition process. After initiation of a special boot

procedure, the examiner uses software to create a "mirror" of the targeted storage. A mirror image of a disk is a "bit level" copy. It includes all information on the disk regardless of whether the computer operating system recognizes the data as an existing file.

To prove that no data has been altered, computer forensic software employs an algorithm to generate an image hash value. The algorithm calculates a numerical value based on the exact contents of the drive that was imaged. If any data on the image changes, even something as little as the addition of a single keystroke or changing the case of a single character, the hash total changes. This provides irrefutable evidence that the data is not altered.

Why Your Information Technology Group Should Not Do this Work.

The emphasis of any computer forensic investigation must be on obtaining unquestioned evidence. Although technical knowledge is certainly required, legal processes, the integrity of evidence, and a clear and concise reporting by an independent expert witness should be the focus. To accomplish your objectives, specific procedures must be followed with specialized software.

Most information technology personnel focus on network administration and user support, rather than the specialized procedures and software that is required to preserve evidence. Even if your in-house personnel had the necessary tools and training, they (i) will be viewed as lacking independence, (ii) will not have the legal-related experience, and (iii) may not be qualified to serve as an expert in computer forensic investigations in court.

Electronic evidence is fragile, and can be easily altered or erased without proper handling. Finding the "smoking gun" will be of little value if you fail to establish that the data was not tampered with or otherwise corrupted. Unless a trained specialist performs the recovery and analysis, the information could be easily destroyed, discredited, or never found. This happens because:

- All files opened by your IT department show an access date/time that proves someone other than the subject employee had access to the critical files. In this situation, it is difficult to establish that the suspect employee was responsible for whatever you find.
- The mere act of turning on a computer, looking at directories and opening files will cause the operating system

especially when compared to the cost of disputes and management distraction.



to write information on the hard drive, thus overwriting information that might otherwise be useful.

- Deleted, disguised, or hidden information is easily overlooked. Some of this information is stored in normally inaccessible areas of the hard drive.

Without specialized software and procedures, valuable evidence will be destroyed or its validity called into question.



In an attempt to avoid the use of specialized software, an in-house solution often involves copying the disk under investigation onto a newly formatted disk. This approach is incomplete. First, a copy made through Windows or DOS will include only those files that the system has been told to “remember”. As a result, data on the disk from “deleted” information, and slack (the data remaining in the unused portion of each sector) will not be included. Second, a reformatted disk continues to house remnants of prior data because the reformatting process does not remove all information from the disk. As a result, data having nothing to do with the investigation will corrupt the results.

Because most companies do not plan to get into a dispute, they rationalize doing the investigation themselves. This is usually a mistake. The reality is that no one “plans” to have a dispute. Our courts are full of cases where the people involved would have preferred to resolve their dispute by dealing with a reasonable adversary. Unfortunately, adversaries often do not see the world the way that you do. The best way of protecting your interests and reaching a settlement is to have strong evidence that supports your position. The vast majority of our clients do not go to court - but that happens because the other side understands the strength of the evidence that they face. If your concerns are important enough to warrant an inspection, it is worth doing the inspection properly.

What Can I Do to Ensure Successful Use of this Information?

Computer data should be part of your proactive HR decisions. You should:

- Obtain an image of computer disks and other storage media used by a departing employee as part of your routine documentation for “difficult” employees. A difficult employee includes anyone (i) whose discharge is likely to be disputed, (ii) likely to raise claims of inappropriate employer conduct, and (iii) leaving to work for a competitor. If this is not done, by the time problems are better known, the former employee’s computer will likely have been passed on to the next user. Through routine ongoing use, the integrity of the evidence from the former employee will be compromised.
- Ensure that your personnel policies communicate expectations regarding the lack of employee privacy when using company computers and electronic systems. Similarly, your policies should include a statement regarding a code of conduct or acceptable use policy with respect to the company’s systems. Employees should confirm their knowledge of these policies, preferably in writing. Most companies already do this as part of their overall HR practices.
- Do not confront the suspect until you have considered covert options. Once an employee is aware of your suspicions, significant electronic information can be deleted or altered by the suspect. Although “deleted” information may be recoverable, do not take that chance. By acting before the suspect makes attempted erasures, covert investigation provides a greater opportunity to collect irrefutable evidence, at an overall lower cost.

Get the advice of legal counsel before performing a covert investigation. You should understand any employee’s rights to privacy.

What Will This Cost and What Reports Will I Receive?

Creation of the disk image is most cost effectively performed in our offices. This simply requires that the disk be unplugged from the computer and sent to us. In this case, our labor charges for creating a mirror image and performing an initial battery of recovery and processing tasks currently costs around **\$1000** (varies slightly based on the type and size of disk).

Our flat fee includes an email report that shows (when such information is available):

- A list of all file names, sizes, extensions, date created, and date last modified for all current files on the disk
- An initial list of the names, sizes, extensions, date created, and date last modified for “deleted” files that perhaps can be recovered
- A list of recent files that were deleted on the system, even if the file cannot be recovered
- An initial list of troubling internet sites visited with this computer sorted by categories (e.g., pornography)
- A list of internet temporary files that remain on the computer
- A listing of certain suspicious software that is not normally part of the software most companies provide to their employees
- Identification of the disk examined along with detailed evidence documentation

As noted earlier, the most cost effective and fastest overall solution is to send the unplugged disk to us. Alternatively, we can bring our equipment to your offices and create an image there. In this case, there are additional charges for travel and the time we are at your location. The copying time depends on the size and speed of the disk we are imaging. Generally, a 20GB disk will take several hours to image. Larger drives are proportionately more time consuming.

If you have specific concerns, we can tailor our search and analysis to meet your specific needs. Our initial report will often highlight areas for potential additional work. You may want to do some inspections yourself, in which case we will send you the relevant files. If you authorize additional work, we bill for this at a competitive hourly rate.

95% of Investigations are Incomplete.

The recent eighth biennial study by Ernst & Young regarding fraud prevention, detection, and investigation included a shocking statistic. Ninety-five percent of formal investigations ignored computerized information and computerized tools. In light of the overwhelming prevalence of computers and the modest cost of gathering electronic evidence, this is inexcusable.

Gathering strong evidence will prevent many disputes from proceeding.

The companies in this survey that used outside consultants provided an amazing show of client satisfaction. Approximately 90% of the companies that used outside forensic auditors were satisfied with the investigation. The wealth of information available from computer forensics can easily determine the outcome of a dispute or potential dispute.

The Fulcrum Advantage

We are not just computer techies. Our firm includes forensic accountants that regularly conduct financial investigations. Our broader expertise allows us to (i) separate the important from the unimportant, and (ii) interpret the results from the overall perspective of your business and its records. By using a single service provider for these related tasks, our work is more complete, better coordinated, and costs less.

Our firm is quite experienced in civil litigation. Should your employee make a claim, or you have a claim of stolen proprietary information, we are well equipped to support your case. Because of this experience, we know how to convert our methodology and conclusions into persuasive information for a judge and jury.

We use updated and sophisticated forensic software. This is important because technology is constantly changing. Our work is of the highest caliber, yet we charge less than the larger firms. You get “big firm” results at a “small firm” price.

**FULCRUM
FINANCIAL
INQUIRY**

© Fulcrum Financial Inquiry LLP

No client engagement or other responsibility exists to recipients of this article. You should consult with your own legal and financial advisors to apply the general guidance herein to your specific situation.

1000 WILSHIRE BLVD SUITE 1650
LOS ANGELES, CA 90017
(213) 787-4100

www.fulcruminquiry.com

**Delivering Championship
Performance in Financial Consulting**