

FORENSIC COMPUTER SERVICE

ELECTRONIC EVIDENCE PROCESSING & ANALYSIS
CIVIL - CRIMINAL - CORPORATE

1374 Clarkson/Clayton Center

#324

Saint Louis, MO. 63011

636-273-4400

314-215-4162 fax

sales@forensic-computerservice.com

http://www.forensic-computerservice.com

Guidelines for Conducting Computer Investigations in the Workplace

When you begin to suspect that current and future information stored on PC's, PDA's, servers and other computer devices may be needed to resolve internal issues or for possible litigation it is important to act immediately and discreetly. Unlike the alteration or shredding of paper files, computer data can be deleted or altered in a manner of seconds. Likewise, CEO's, managers and supervisors typically don't have the technical ability to accurately back up or otherwise preserve data in a method likely to go unchallenged. Company management typically relies on their IT staff or in smaller organizations, outside technicians or consultants, to perform these type of tasks which use retail software that does not save the entire disc. There is an element of risk involved when using internal staff. Several issues we have encountered include (1) The IT staff could alert others within the organization when an unusual request is made by management; (2) The IT staff are typically inquisitive by nature and questions asked to management which go unanswered may be taken as red flags of "something's up"; (3) An IT employee may be best buddies with the subject of your request and tips him or her off.

An interesting case involved an accounts payable clerk who was suspected of processing invoices for a fake company and having checks processed and mailed.

The clerk was alerted when another employee in charge of backing up the data on her PC told the clerk that management requested a backup of her computer. Although the clerk was not technically competent to delete or alter computer data, her boyfriend was a senior level systems engineer for a technology company and one evening, after business hours, they both entered the premises. The boyfriend not only removed incriminating data off her PC but also gained access to the corporate network server and backup tapes even though what we consider to be "average" security measures had been taken by the IT staff to secure the company networks and data. Backup data was easily erased by waving a \$15.00 magnet over the tapes and A/P network data files were altered to the point of corruption and rendered unreadable.

Such tactics are not uncommon when a desperate employee is faced with possible criminal action. These acts not only destroyed important electronic evidence but also caused an operating disruption and financial hardship to the company for three months while the data was reconstructed manually.

There are several practical reasons for using a third party to acquire and analyze data. First, the third party is trained and experienced in this type of work. FCS uses an analytical approach to acquiring data, meaning we create an exact image of the subject's storage media. By using this method we can always exclude data which doesn't apply while avoiding the situation where the circumstances change down the road and suddenly you need additional files but find out they are now permanently gone off the subject's computer. Second, FCS uses acquisition software which methods have been proven and upheld in trial and appellate courts. Third, matters involving computer data which proceed to litigation are realistically subject to the "evidence tainting" accusation. This can open up a large can of worms when your own staff acquired the data and stored it internally. *Who had access ?, How do we know this data wasn't altered ?, Isn't it true you disliked the subject ?* are just a few of the questions raised. In the end it may cost you more money in depositions, testimony, lost productivity and morale than it would to use a third party, professional service.

Company X used their internal staff to copy existing data from an employee's computer where they suspected pornographic pictures had been saved. Management found over 150 pornographic pictures stored on the employee's hard drive. The employee was immediately terminated for having downloaded and saved pornographic material using the company network and equipment.

The employee sued the company and denied having any pornographic material on his computer. FCS was granted access to the company computer used by the employee. What appeared to be a nailed-shut case suddenly took an opposite turn. FCS determined and proved that the employee's computer had become infected with a worm which downloaded pictures from known, pornographic web sites. This worm worked in such a way that even a well trained computer user would have absolutely no clue as to what was being accessed and downloaded to their PC.

Even with overwhelming evidence there may be other evidence hidden and thus overlooked by others. FCS looks at all possibilities to provide our clients with accurate reporting.

IMPORTANT CONSIDERATIONS

1. Time is critical

Computer data can be altered and erased quickly. Take action as soon as possible to preserve all data on the subject computer. Many times this can be done after hours when the subject is unaware of what is taking place. Consider using FCS's Rapid Response service for locations in the midwest which require immediate attention.

2. Operate in stealth mode

Use a qualified, third party company to preserve and analyze the data. Keep discussions regarding the issue on a "need to know" basis. Gossip travels fast, faster in large corporations, and, faster than the Internet !

3. Defer employee termination

Depending on the issues and circumstances, defer termination of the subject employee(s) until the data can be acquired and analyzed. Base your future action on the analysis report as well as other factors pertaining to the subject's job, performance and other criteria as you would for any employee. Sometimes what you initially see is not the complete picture and may lead to claims against by the employee against the company.

4. Document everything

If you are using internal IT staff to acquire data ensure that the acquisition is well documented with "who, what, when, where and how". Have at least one copy of the data made and kept off-site with counsel, a lock box or other safe location.

5. Consult with an attorney

Depending on the circumstance and issues, consult with legal counsel before taking action. As we mentioned earlier there have been cases with what appeared to be undisputable evidence, only to find out later (with less change in your pocket) differently.

6. Consider monitoring the employee

In cases where data is acquired and the investigation is ongoing, FCS can assist you with special software and tools to closely monitor and log the employee's computer usage, without their knowledge, to obtain additional evidence in building your case. We suggest that you consult with legal counsel before deploying "spyware" as your company policies, state and federal laws may interfere with your ability to obtain and/or use such evidence.

7. Establish and maintain a policy

Create and review a computer usage policy for your company. You may want to consult with your legal counsel for help in wording a good policy for your employees. We suggest being broad in scope by using a phrase like "computing equipment" instead of "personal computer".